



Australian Government  
Department of Home Affairs



CRITICAL  
INFRASTRUCTURE  
CENTRE

A large circular graphic with an orange border, containing a blurred image of a modern infrastructure tunnel or road with blue and white lighting. The text is centered within this circle.

# Security Legislation Amendment (Critical Infrastructure) Bill 2020

Exposure Draft

November 2020

# EXPOSURE DRAFT

2019-2020

The Parliament of the  
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

EXPOSURE DRAFT
----------------

## **Security Legislation Amendment (Critical Infrastructure) Bill 2020**

**No.     , 2020**

*(Home Affairs)*

**A Bill for an Act to amend legislation relating to  
critical infrastructure, and for other purposes**

# EXPOSURE DRAFT

# EXPOSURE DRAFT

---

## Contents

1	Short title.....	1
2	Commencement.....	1
3	Schedules.....	2
<b>Schedule 1—Security of critical infrastructure</b>		<b>4</b>
Part 1—General amendments		4
<i>Administrative Decisions (Judicial Review) Act 1977</i>		4
<i>AusCheck Act 2007</i>		4
<i>Security of Critical Infrastructure Act 2018</i>		4
Part 2—Application provisions		132
Part 3—Amendments contingent on the commencement of the Federal Circuit and Family Court of Australia Act 2020		133
<i>Security of Critical Infrastructure Act 2018</i>		133
<b>Schedule 2—Australian Signals Directorate</b>		<b>134</b>
<i>Criminal Code Act 1995</i>		134



# EXPOSURE DRAFT

1     **A Bill for an Act to amend legislation relating to**  
2     **critical infrastructure, and for other purposes**

3     The Parliament of Australia enacts:

4     **1 Short title**

5                     This Act is the *Security Legislation Amendment (Critical*  
6                     *Infrastructure) Act 2020*.

7     **2 Commencement**

8                     (1) Each provision of this Act specified in column 1 of the table  
9                     commences, or is taken to have commenced, in accordance with  
10                    column 2 of the table. Any other statement in column 2 has effect  
11                    according to its terms.  
12

# EXPOSURE DRAFT

---

---

## 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. Schedule 1, Parts 1 and 2	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 6 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	
3. Schedule 1, Part 3	The later of: (a) immediately after the commencement of the provisions covered by table item 2; and (b) the commencement of the <i>Federal Circuit and Family Court of Australia Act 2020</i> .  However, the provisions do not commence at all if the event mentioned in paragraph (b) does not occur.	
4. Schedule 2	The day after this Act receives the Royal Assent.	

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

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

### 3 Schedules

8 Legislation that is specified in a Schedule to this Act is amended or  
9 repealed as set out in the applicable items in the Schedule

# EXPOSURE DRAFT

---

1 concerned, and any other item in a Schedule to this Act has effect  
2 according to its terms.

# EXPOSURE DRAFT

Schedule 1 Security of critical infrastructure

Part 1 General amendments

---

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

2 **Part 1—General amendments**

3 *Administrative Decisions (Judicial Review) Act 1977*

4 **1 Before paragraph (da) of Schedule 1**

5 Insert:

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

8 *AusCheck Act 2007*

9 **2 Subsection 4(1)**

10 Insert:

11 *critical infrastructure risk management program* has the same  
12 meaning as in the *Security of Critical Infrastructure Act 2018*.

13 **3 After paragraph 8(1)(b)**

14 Insert:

15 (ba) critical infrastructure risk management programs are  
16 required, by rules made under the *Security of Critical*  
17 *Infrastructure Act 2018*, to include provisions that require  
18 background checks of individuals to be conducted under the  
19 AusCheck scheme; or

20 *Security of Critical Infrastructure Act 2018*

21 **4 Section 3**

22 Omit “to national security”.

23 **5 At the end of section 3**

24 Add:

25 ; and (c) requiring responsible entities for critical infrastructure assets  
26 to identify and manage risks relating to those assets; and

---



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (d) providing a regime for the Commonwealth to respond to  
2 serious cyber security incidents; and  
3 (e) imposing enhanced cyber security obligations on responsible  
4 entities for systems of national significance in order to  
5 improve their preparedness for, and ability to respond to,  
6 cyber security incidents.

## 7 **6 Section 4**

8 Repeal the section, substitute:

### 9 **4 Simplified outline of this Act**

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

12 The framework consists of the following:

- 13 (a) the keeping of a register of information in relation to  
14 critical infrastructure assets (the register will not be  
15 made public);  
16 (b) requiring the responsible entity for one or more critical  
17 infrastructure assets to have, and comply with, a critical  
18 infrastructure risk management program;  
19 (c) requiring notification of cyber security incidents;  
20 (d) imposing enhanced cyber security obligations that relate  
21 to systems of national significance;  
22 (e) requiring certain entities relating to a critical  
23 infrastructure asset to provide information in relation to  
24 the asset, and to notify if certain events occur in relation  
25 to the asset;  
26 (f) allowing the Minister to require certain entities relating  
27 to a critical infrastructure asset to do, or refrain from  
28 doing, an act or thing if the Minister is satisfied that  
29 there is a risk of an act or omission that would be  
30 prejudicial to security;  
31 (g) allowing the Secretary to require certain entities relating  
32 to a critical infrastructure asset to provide certain  
33 information or documents;

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23

- (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 Minister may privately declare a critical infrastructure asset to be a system of national significance.

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

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (b) in a case where the computer data is held in a computer—the  
2 copying or moving of the data to:  
3 (i) any other location in the computer; or  
4 (ii) another computer; or  
5 (iii) a data storage device; or  
6 (c) in a case where the computer data is held in a data storage  
7 device—the copying or moving of the data to:  
8 (i) a computer; or  
9 (ii) another data storage device.

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

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

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

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

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

19 ***asset*** includes:

- 20 (a) a system; and  
21 (b) a network; and  
22 (c) a facility; and  
23 (d) a computer; and  
24 (e) a computer device; and  
25 (f) a computer program; and  
26 (g) computer data; and  
27 (h) premises; and  
28 (i) any other thing.

29 ***associated transmission facility*** means:

- 30 (a) an antenna; or  
31 (b) a combiner; or  
32 (c) a feeder system; or  
33 (d) an apparatus; or
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (e) an item of equipment; or  
2 (f) a structure; or  
3 (g) a line; or  
4 (h) an electricity cable or wire;  
5 that is associated with a radiocommunications transmitter.

6 ***AusCheck scheme*** has the same meaning as in the *AusCheck Act*  
7 *2007*.

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

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

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

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

16 ***authorised agency*** means ASD.

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

19 ***background check*** has the same meaning as in the *AusCheck Act*  
20 *2007*.

21 ***banking business*** has the same meaning as in the *Banking Act*  
22 *1959*.

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

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

27 ***broadcasting transmission asset*** means:

- 28 (a) a radiocommunications transmitter; or  
29 (b) a broadcasting transmission tower; or  
30 (c) an associated transmission facility;

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

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

- 3 (d) a national broadcasting service; or
- 4 (e) a commercial radio broadcasting service; or
- 5 (f) a commercial television broadcasting service.

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

8 ***business critical data*** means:

- 9 (a) personal information (within the meaning of the *Privacy Act*  
10 *1988*) that relates to at least 20,000 individuals; or
- 11 (b) sensitive information (within the meaning of the *Privacy Act*  
12 *1988*); or
- 13 (c) information relating to any research and development in  
14 relation to a critical infrastructure asset; or
- 15 (d) information relating to any systems needed to operate a  
16 critical infrastructure asset; or
- 17 (e) information relating to risk management and business  
18 continuity (however described) in relation to a critical  
19 infrastructure asset.

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

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

24 ***carrier*** has the same meaning as in the *Telecommunications Act*  
25 *1997*.

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

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

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

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

---

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1                    **communication passing over a telecommunications system** has  
2                    the same meaning as in the *Telecommunications (Interception and*  
3                    *Access) Act 1979*.

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

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

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

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

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

- 19                   (a) a computer; or
- 20                   (b) a data storage device.

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

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

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

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

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

31                   **critical aviation asset** means:

- 32                   (a) an asset that:
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (i) is used in connection with the provision of an air  
2 service; and  
3 (ii) is owned or operated by an aircraft operator; or  
4 (b) an asset that:  
5 (i) is used in connection with the provision of an air  
6 service; and  
7 (ii) is owned or operated by a regulated air cargo agent; or  
8 (c) an asset that is used by an airport operator in connection with  
9 the operation of an airport.

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

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

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

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

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

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

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

22 ***critical defence capability*** includes:

- 23 (a) materiel; and  
24 (b) technology; and  
25 (c) a platform; and  
26 (d) a network; and  
27 (e) a system; and  
28 (f) a service;

29 that is required in connection with:

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

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 (a) is being, or will be, supplied by an entity to the Defence  
2 Department, or the Australian Defence Force, under a  
3 contract; and

4 (b) consists of, or enables, a critical defence capability.

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

7 ***critical domain name system*** means a system that:

8 (a) is owned by an entity that is the subject of a determination  
9 under subsection 474(1) of the *Telecommunications Act*  
10 *1997*; and

11 (b) is used to administer an Australian domain name system.

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

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

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

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

20 (a) is used by:

21 (i) Australian Energy Market Operator Limited  
22 (ACN 072 010 327); or

23 (ii) Power and Water Corporation; or

24 (iii) Regional Power Corporation; or

25 (iv) Electricity Networks Corporation; and

26 (b) is critical to ensuring the security and reliability of an energy  
27 market.

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

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

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

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

---



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

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

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

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

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

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

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

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

15 ***critical infrastructure risk management program*** has the meaning  
16 given by section 30AH.

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

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

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

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

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

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

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

- 28 (a) is managed by a single entity; and  
29 (b) is capable of handling at least 5 million passenger journeys  
30 per month.

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

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

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

5                    **critical telecommunications asset** means:

6                    (a) a telecommunications network that is:

7                    (i) owned or operated by a carrier; and

8                    (ii) used to supply a carriage service; or

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

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

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

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

14                    **cyber security exercise** has the meaning given by section 30CN.

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

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

17                    **data storage** includes data back-up.

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

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

24                    **data storage or processing sector** means the sector of the  
25                    Australian economy that involves providing data storage or  
26                    processing services on a commercial basis.

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

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

29                    (b) a data processing service.

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

---

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1            **defence industry sector** means the sector of the Australian  
2            economy that involves the provision of critical defence  
3            capabilities.
- 4            **Defence Minister** means the Minister administering section 1 of  
5            the *Defence Act 1903*.
- 6            **derivative trade repository** has the same meaning as in Chapter 7  
7            of the *Corporations Act 2001*.
- 8            **designated officer** has the meaning given by section 30DQ.
- 9            **Electricity Networks Corporation** means the Electricity Networks  
10           Corporation established by section 4 of the *Electricity*  
11           *Corporations Act 2005* (WA).
- 12           **electronic communication** means a communication of information  
13           in any form by means of guided or unguided electromagnetic  
14           energy.
- 15           **energy sector** means the sector of the Australian economy that  
16           involves:  
17           (a) the production, distribution or supply of electricity; or  
18           (b) the production, processing, distribution or supply of gas; or  
19           (c) the production, processing, distribution or supply of liquid  
20           fuel.
- 21           **engage in conduct** means:  
22           (a) do an act; or  
23           (b) omit to perform an act.
- 24           **evaluation report** has the meaning given by section 30CS.
- 25           **external auditor** means a person authorised under section 30CT to  
26           be an external auditor for the purposes of this Act.
- 27           **financial benchmark** has the same meaning as in Part 7.5B of the  
28           *Corporations Act 2001*.
- 29           **financial market** has the same meaning as in Chapter 7 of the  
30           *Corporations Act 2001*.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

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

- 3 (a) carrying on banking business; or  
4 (b) operating a superannuation fund; or  
5 (c) carrying on insurance business; or  
6 (d) carrying on life insurance business; or  
7 (e) carrying on health insurance business; or  
8 (f) operating a financial market; or  
9 (g) operating a clearing and settlement facility;  
10 (h) operating a derivative trade repository; or  
11 (i) administering a financial benchmark; or  
12 (j) operating a payment system; or  
13 (k) carrying on financial services business; or  
14 (l) carrying on credit facility business.

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

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

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

- 20 (a) manufacturing; or  
21 (b) processing; or  
22 (c) packaging; or  
23 (d) distributing; or  
24 (e) supplying;

25 food or groceries on a commercial basis.

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

- 27 (a) is in a gaseous state at standard temperature and pressure;  
28 and  
29 (b) consists of naturally occurring hydrocarbons, or a naturally  
30 occurring mixture of hydrocarbons and non-hydrocarbons,  
31 the principal constituent of which is methane; and  
32 (c) is suitable for consumption.

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

---

# EXPOSURE DRAFT

- 1 (a) is equipped and staffed so that it is capable of providing to a  
2 patient:  
3 (i) mechanical ventilation for a period of several days; and  
4 (ii) invasive cardiovascular monitoring; and  
5 (b) is supported by:  
6 (i) during normal working hours—at least one specialist, or  
7 consultant physician, in the specialty of intensive care,  
8 who is immediately available, and exclusively rostered,  
9 to that area; and  
10 (ii) at all times—at least one medical practitioner who is  
11 present in the hospital and immediately available to that  
12 area; and  
13 (iii) at least 18 hours each day—at least one nurse; and  
14 (c) has admission and discharge policies in operation.

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

17 **health care** includes:

- 18 (a) services provided by individuals who practise in any of the  
19 following professions or occupations:  
20 (i) dental (including the profession of a dentist, dental  
21 therapist, dental hygienist, dental prosthetist and oral  
22 health therapist);  
23 (ii) medical;  
24 (iii) medical radiation practice;  
25 (iv) nursing;  
26 (v) midwifery;  
27 (vi) occupational therapy;  
28 (vii) optometry;  
29 (viii) pharmacy;  
30 (ix) physiotherapy;  
31 (x) podiatry;  
32 (xi) psychology;  
33 (xii) a profession or occupation specified in the rules; and  
34 (b) treatment and maintenance as a patient at a hospital.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

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

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

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

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

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

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

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

19 **IGIS official** means:

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

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

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

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

30 **incident response plan** has the meaning given by section 30CJ.

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

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 *insurance business* has the same meaning as in the *Insurance Act*  
2 *1973*.

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

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

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

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

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

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

- 15 (a) manages:
- 16 (i) the asset; or
- 17 (ii) a part of the asset; or
- 18 (b) manages an aspect of:
- 19 (i) the asset; or
- 20 (ii) a part of the asset; or
- 21 (c) manages an aspect of the operation of:
- 22 (i) the asset; or
- 23 (ii) a part of the asset.

24 *medical supplies* includes:

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

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

29 *modification*:

- 30 (a) in respect of computer data—means:
- 31 (i) the alteration or removal of the data; or
- 32 (ii) an addition to the data; or

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

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

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

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

9 ***notification provision*** means:

- 10 (a) subsection 35AE(3); or  
11 (b) subsection 35AE(4); or  
12 (c) subsection 35AE(5); or  
13 (d) subsection 35AE(6); or  
14 (e) subsection 35AE(7); or  
15 (f) subsection 35AE(8); or  
16 (g) subsection 35AH(5); or  
17 (h) subsection 35AH(6); or  
18 (i) subsection 35AH(7); or  
19 (j) subsection 35AY(3); or  
20 (k) subsection 35AY(4); or  
21 (l) subsection 35AY(5); or  
22 (m) subsection 35AY(6); or  
23 (n) subsection 35AY(7); or  
24 (o) subsection 35AY(8); or  
25 (p) subsection 51(3); or  
26 (q) subsection 52(4); or  
27 (r) subsection 52B(3); or  
28 (s) subsection 52D(4).

29 ***Ombudsman official*** means:

- 30 (a) the Ombudsman; or  
31 (b) a Deputy Commonwealth Ombudsman; or  
32 (c) a person who is a member of the staff referred to in  
33 subsection 31(1) of the *Ombudsman Act 1976*.



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 **8 Section 5 (paragraph (b) of the definition of *operator*)**

2 Repeal the paragraph, substitute:

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

5 **9 Section 5**

6 Insert:

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

9 **10 Section 5**

10 Insert:

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

14 **11 Section 5 (after paragraph (b) of the definition of *protected***  
15 ***information*)**

16 Insert:

- 17 (ba) records or is the fact that an asset is declared under  
18 section 52B to be a system of national significance; or  
19 (bb) records or is the fact that the Minister has:  
20 (i) given a Ministerial authorisation; or  
21 (ii) revoked a Ministerial authorisation; or  
22 (bc) is, or is included in, a critical infrastructure risk management  
23 program that is adopted by an entity in compliance with  
24 section 30AC; or  
25 (bd) is, or is included in, a report that is given under  
26 section 30AG; or  
27 (be) is, or is included in, a report under section 30BC or 30BD; or  
28 (bf) is, or is included in, an incident response plan adopted by an  
29 entity in compliance with section 30CD; or  
30 (bg) is, or is included in, an evaluation report prepared under  
31 section 30CQ or 30CR; or  
32 (bh) is, or is included in, a vulnerability assessment report  
33 prepared under section 30CZ; or

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (bi) is, or is included in, a report prepared in compliance with:  
2 (i) a system information periodic reporting notice; or  
3 (ii) a system information event-based reporting notice; or  
4 (bj) records or is the fact that the Secretary has:  
5 (i) given a direction under section 35AK; or  
6 (ii) revoked such a direction; or  
7 (bk) records or is the fact that the Secretary has:  
8 (i) given a direction under section 35AQ; or  
9 (ii) revoked such a direction; or  
10 (bl) records or is the fact that the Secretary has:  
11 (i) given a request under section 35AX; or  
12 (ii) revoked such a request; or

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

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

### 17 13 Section 5

18 Insert:

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

21 *regional centre* means a city, or a town, that has a population of  
22 10,000 or more people.

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

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

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

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

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1                    *relevant Commonwealth regulator* means:  
2                    (a) a Department that is specified in the rules; or  
3                    (b) a body that is:  
4                        (i) established by a law of the Commonwealth; and  
5                        (ii) specified in the rules.

- 6                    *relevant entity*, in relation to an asset, means an entity that:  
7                    (a) is the responsible entity for the asset; or  
8                    (b) is a direct interest holder in relation to the asset; or  
9                    (c) is an operator of the asset; or  
10                   (d) is a managed service provider for the asset.

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

## 12    **14 Section 5 (definition of *relevant industry*)**

13                   Repeal the definition.

## 14    **15 Section 5 (definition of *responsible entity*)**

15                   Repeal the definition, substitute:

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

## 18    **16 Section 5 (paragraph (a) of the definition of *security*)**

19                   Omit “10 and 12”, substitute “10, 12, 12A, 12M, 12N and 30AG”.

## 20    **17 Section 5 (paragraph (b) of the definition of *security*)**

21                   Omit “10 and 12”, substitute “10, 12, 12A, 12M, 12N and 30AG”.

## 22    **18 Section 5**

23                   Insert:

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

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

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

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

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

12 **system information event-based reporting notice** means a notice  
13 under subsection 30DC(2).

14 **system information periodic reporting notice** means a notice under  
15 subsection 30DB(2).

16 **system information software notice** means a notice under  
17 subsection 30DJ(2).

18 **system of national significance** has the meaning given by  
19 section 52B.

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

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

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

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

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

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

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (a) owning or operating assets that are used in connection with  
2 the transport of goods or passengers on a commercial basis;  
3 or  
4 (b) the transport of goods or passengers on a commercial basis.

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

7 ***vulnerability assessment*** has the meaning given by section 30CY.

8 ***vulnerability assessment report*** has the meaning given by  
9 section 30DA.

10 ***water and sewerage sector*** means the sector of the Australian  
11 economy that involves operating water or sewerage systems or  
12 networks.

## 13 **19 Section 5 (definition of *water utility*)**

14 After “water services”, insert “or sewerage services, or both”.

## 15 **20 At the end of section 6**

16 Add:

17 *Interest and control information provided by the Commonwealth*

- 18 (5) If the first entity:  
19 (a) is the Governor-General, the Prime Minister or a Minister;  
20 and  
21 (b) is a direct interest holder in relation to an asset because of  
22 paragraph 8(1)(b);  
23 the first entity is not required to provide any interest and control  
24 information.

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

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 **21 After section 8C**

2 Insert:

3 **8D Meaning of *critical infrastructure sector***

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

- 6 (a) the communications sector;  
7 (b) the data storage or processing sector;  
8 (c) the financial services and markets sector;  
9 (d) the water and sewerage sector;  
10 (e) the energy sector;  
11 (f) the health care and medical sector;  
12 (g) the higher education and research sector;  
13 (h) the food and grocery sector;  
14 (i) the transport sector;  
15 (j) the space technology sector;  
16 (k) the defence industry sector.

17 **8E Meaning of *critical infrastructure sector asset***

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

20 *Deeming—when asset relates to a sector*

21 (2) For the purposes of this Act, each of the following assets is taken  
22 to relate to the communications sector:

- 23 (a) a critical telecommunications asset;  
24 (b) a critical broadcasting asset;  
25 (c) a critical domain name system.

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

28 (4) For the purposes of this Act, each of the following assets is taken  
29 to relate to the financial services and markets sector:

- 30 (a) a critical banking asset;  
31 (b) a critical superannuation asset;
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (c) a critical insurance asset;  
2 (d) a critical financial market infrastructure asset.
- 3 (5) For the purposes of this Act, a critical water asset is taken to relate  
4 to the water and sewerage sector.
- 5 (6) For the purposes of this Act, each of the following assets is taken  
6 to relate to the energy sector:  
7 (a) a critical electricity asset;  
8 (b) a critical gas asset;  
9 (c) a critical energy market operator asset;  
10 (d) a critical liquid fuel asset.
- 11 (7) For the purposes of this Act, a critical hospital is taken to relate to  
12 the health care and medical sector.
- 13 (8) For the purposes of this Act, a critical education asset is taken to  
14 relate to the higher education and research sector.
- 15 (9) For the purposes of this Act, a critical food and grocery asset is  
16 taken to relate to the food and grocery sector.
- 17 (10) For the purposes of this Act, each of the following assets is taken  
18 to relate to the transport sector:  
19 (a) a critical port;  
20 (b) a critical freight infrastructure asset;  
21 (c) a critical freight services asset;  
22 (d) a critical public transport asset;  
23 (e) a critical aviation asset.
- 24 (11) For the purposes of this Act, a critical defence industry asset is  
25 taken to relate to the defence industry sector.

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

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

#### 1 **8G Meaning of *relevant impact***

- 2 (1) Each of the following is a ***relevant impact*** of a hazard on a critical  
3 infrastructure asset:
- 4 (a) the impact (whether direct or indirect) of the hazard on the  
5 availability of the asset;
  - 6 (b) the impact (whether direct or indirect) of the hazard on the  
7 integrity of the asset;
  - 8 (c) the impact (whether direct or indirect) of the hazard on the  
9 reliability of the asset;
  - 10 (d) the impact (whether direct or indirect) of the hazard on the  
11 confidentiality of:
    - 12 (i) information about the asset; or
    - 13 (ii) if information is stored in the asset—the information; or
    - 14 (iii) if the asset is computer data—the computer data.
- 15 (2) Each of the following is a ***relevant impact*** of a cyber security  
16 incident on a critical infrastructure asset:
- 17 (a) the impact (whether direct or indirect) of the incident on the  
18 availability of the asset;
  - 19 (b) the impact (whether direct or indirect) of the incident on the  
20 integrity of the asset;
  - 21 (c) the impact (whether direct or indirect) of the incident on the  
22 reliability of the asset;
  - 23 (d) the impact (whether direct or indirect) of the incident on the  
24 confidentiality of:
    - 25 (i) information about the asset; or
    - 26 (ii) if information is stored in the asset—the information; or
    - 27 (iii) if the asset is computer data—the computer data.
- 28 (3) Each of the following is a ***relevant impact*** of a cyber security  
29 incident on a system of national significance:
- 30 (a) the impact (whether direct or indirect) of the incident on the  
31 availability of the system;
  - 32 (b) the impact (whether direct or indirect) of the incident on the  
33 integrity of the system;
  - 34 (c) the impact (whether direct or indirect) of the incident on the  
35 reliability of the system;
-



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (d) the impact (whether direct or indirect) of the incident on the  
2 confidentiality of:  
3 (i) information about the system; or  
4 (ii) if information is stored in the system—the information;  
5 or  
6 (iii) if the system is computer data—the computer data.

## 7 **22 Paragraphs 9(1)(a), (b), (c) and (d)**

8 Repeal the paragraphs, substitute:

- 9 (a) a critical telecommunications asset; or  
10 (b) a critical broadcasting asset; or  
11 (c) a critical domain name system; or  
12 (d) a critical data storage or processing asset; or  
13 (da) a critical banking asset; or  
14 (db) a critical superannuation asset; or  
15 (dc) a critical insurance asset; or  
16 (dd) a critical financial market infrastructure asset; or  
17 (de) a critical water asset; or  
18 (df) a critical electricity asset; or  
19 (dg) a critical gas asset; or  
20 (dh) a critical energy market operator asset; or  
21 (di) a critical liquid fuel asset; or  
22 (dj) a critical hospital; or  
23 (dk) a critical education asset; or  
24 (dl) a critical food and grocery asset; or  
25 (dm) a critical port; or  
26 (dn) a critical freight infrastructure asset; or  
27 (do) a critical freight services asset; or  
28 (dp) a critical public transport asset; or  
29 (dq) a critical aviation asset; or  
30 (dr) a critical defence industry asset; or

## 31 **23 At the end of subsection 9(1)**

32 Add:

33 Note: For prescription by class, see subsection 13(3) of the *Legislation Act*  
34 *2003*.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

#### 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

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (b) a body corporate established by a law of the Commonwealth  
2 (other than a government business enterprise);  
3 the asset is not a critical infrastructure asset unless:  
4 (c) the asset is declared under section 51 to be a critical  
5 infrastructure asset; or  
6 (d) the asset is prescribed by the rules for the purposes of  
7 paragraph (1)(f).
- 8 (2B) An asset is not a critical infrastructure asset to the extent to which  
9 the asset is located outside Australia.

## 10 **27 Paragraph 9(3)(b)**

- 11 Repeal the paragraph, substitute:  
12 (b) the asset relates to a critical infrastructure sector.

## 13 **28 Subparagraph 9(4)(a)(i)**

- 14 Before “located”, insert “wholly or partly”.

## 15 **29 Subparagraph 9(4)(a)(ii)**

- 16 Omit “industry for the asset”, substitute “critical infrastructure sector”.

## 17 **30 Paragraph 10(1)(a)**

- 18 After “customers”, insert “or any other number of customers prescribed  
19 by the rules”.

## 20 **31 Paragraph 12(1)(b)**

- 21 Repeal the paragraph, substitute:  
22 (b) a gas storage facility that has a maximum daily withdrawal  
23 capacity of at least 75 terajoules per day or any other  
24 maximum daily withdrawal capacity prescribed by the rules;

## 25 **32 After section 12**

- 26 Insert:

## 27 **12A Meaning of *critical liquid fuel asset***

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (a) a liquid fuel refinery that is critical to ensuring the security  
2 and reliability of a liquid fuel market, in accordance with  
3 subsection (2);
- 4 (b) a liquid fuel pipeline that is critical to ensuring the security  
5 and reliability of a liquid fuel market, in accordance with  
6 subsection (3);
- 7 (c) a liquid fuel storage facility that is critical to ensuring the  
8 security and reliability of a liquid fuel market, in accordance  
9 with subsection (4).
- 10 Note: The rules may prescribe that a specified critical liquid fuel asset is not  
11 a critical infrastructure asset (see section 9).
- 12 (2) For the purposes of paragraph (1)(a), the rules may prescribe:
- 13 (a) specified liquid fuel refineries that are critical to ensuring the  
14 security and reliability of a liquid fuel market; or
- 15 (b) requirements for a liquid fuel refinery to be critical to  
16 ensuring the security and reliability of a liquid fuel market.
- 17 (3) For the purposes of paragraph (1)(b), the rules may prescribe:
- 18 (a) specified liquid fuel pipelines that are critical to ensuring the  
19 security and reliability of a liquid fuel market; or
- 20 (b) requirements for a liquid fuel pipeline to be critical to  
21 ensuring the security and reliability of a liquid fuel market.
- 22 (4) For the purposes of paragraph (1)(c), the rules may prescribe:
- 23 (a) specified liquid fuel storage facilities that are critical to  
24 ensuring the security and reliability of a liquid fuel market; or
- 25 (b) requirements for a liquid fuel storage facility to be critical to  
26 ensuring the security and reliability of a liquid fuel market.

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

- 27
- 28 (1) An asset is a *critical freight infrastructure asset* if it is any of the  
29 following:
- 30 (a) a road network that, in accordance with subsection (2),  
31 functions as a critical corridor for the transportation of goods  
32 between:
- 33 (i) 2 States; or  
34 (ii) a State and a Territory; or

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (iii) 2 Territories; or  
2 (iv) 2 regional centres;  
3 (b) a rail network that, in accordance with subsection (3),  
4 functions as a critical corridor for the transportation of goods  
5 between:  
6 (i) 2 States; or  
7 (ii) a State and a Territory; or  
8 (iii) 2 Territories; or  
9 (iv) 2 regional centres;  
10 (c) an intermodal transfer facility that, in accordance with  
11 subsection (4), is critical to the transportation of goods  
12 between:  
13 (i) 2 States; or  
14 (ii) a State and a Territory; or  
15 (iii) 2 Territories; or  
16 (iv) 2 regional centres.

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

- 19 (2) For the purposes of paragraph (1)(a), the rules may prescribe:  
20 (a) specified road networks that function as a critical corridor for  
21 the transportation of goods between:  
22 (i) 2 States; or  
23 (ii) a State and a Territory; or  
24 (iii) 2 Territories; or  
25 (iv) 2 regional centres; or  
26 (b) requirements for a road network to function as a critical  
27 corridor for the transportation of goods between:  
28 (i) 2 States; or  
29 (ii) a State and a Territory; or  
30 (iii) 2 Territories; or  
31 (iv) 2 regional centres.
- 32 (3) For the purposes of paragraph (1)(b), the rules may prescribe:  
33 (a) specified rail networks that function as a critical corridor for  
34 the transportation of goods between:  
35 (i) 2 States; or

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (ii) a State and a Territory; or  
2 (iii) 2 Territories; or  
3 (iv) 2 regional centres; or  
4 (b) requirements for a rail network to function as a critical  
5 corridor for the transportation of goods between:  
6 (i) 2 States; or  
7 (ii) a State and a Territory; or  
8 (iii) 2 Territories; or  
9 (iv) 2 regional centres.
- 10 (4) For the purposes of paragraph (1)(c), the rules may prescribe:  
11 (a) specified intermodal transfer facilities that are critical to the  
12 transportation of goods between:  
13 (i) 2 States; or  
14 (ii) a State and a Territory; or  
15 (iii) 2 Territories; or  
16 (iv) 2 regional centres; or  
17 (b) requirements for an intermodal transfer facility to be critical  
18 to the transportation of goods between:  
19 (i) 2 States; or  
20 (ii) a State and a Territory; or  
21 (iii) 2 Territories; or  
22 (iv) 2 regional centres.
- 23 (5) For the purposes of this section, *road network* includes a part of a  
24 road network.
- 25 (6) For the purposes of this section, *rail network* includes a part of a  
26 rail network.

#### 27 **12C Meaning of *critical freight services asset***

- 28 (1) An asset is a *critical freight services asset* if it is a network that is  
29 used by an entity carrying on a business that, in accordance with  
30 subsection (2), is critical to the transportation of goods by any or  
31 all of the following:  
32 (a) road;  
33 (b) rail;
-

# EXPOSURE DRAFT

- 1 (c) inland waters;  
2 (d) sea.

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

- 5 (2) For the purposes of subsection (1), the rules may prescribe:  
6 (a) specified businesses that are critical to the transportation of  
7 goods any or all of the following:  
8 (i) road;  
9 (ii) rail;  
10 (iii) inland waters;  
11 (iv) sea; or  
12 (b) requirements for a business to be critical to the transportation  
13 of goods by any or all of the following:  
14 (i) road;  
15 (ii) rail;  
16 (iii) inland waters;  
17 (iv) sea.

## 18 **12D Meaning of *critical financial market infrastructure asset***

- 19 (1) An asset is a ***critical financial market infrastructure asset*** if it is  
20 any of the following assets:  
21 (a) an asset that:  
22 (i) is owned or operated by an Australian body corporate  
23 that holds an Australian market licence; and  
24 (ii) is critical to the operation of a financial market, in  
25 accordance with subsection (2).  
26 (b) an asset that:  
27 (i) is owned or operated by a body corporate that is a  
28 related body corporate of an Australian body corporate  
29 that holds an Australian market licence; and  
30 (ii) is critical to the operation of a financial market, in  
31 accordance with subsection (2).  
32 (c) an asset that:  
33 (i) is owned or operated by an Australian body corporate  
34 that holds an Australian CS facility licence; and

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (ii) is critical to the operation of a clearing and settlement  
2 facility, in accordance with subsection (3);
- 3 (d) an asset that:
- 4 (i) is owned or operated by a body corporate that is a  
5 related body corporate of an Australian body corporate  
6 that holds an Australian CS facility licence; and
- 7 (ii) is critical to the operation of a clearing and settlement  
8 facility, in accordance with subsection (3);
- 9 (e) an asset that:
- 10 (i) is owned or operated by an Australian body corporate  
11 that holds a benchmark administrator licence; and
- 12 (ii) is critical to the administration of a significant financial  
13 benchmark, in accordance with subsection (4);
- 14 (f) an asset that:
- 15 (i) is owned or operated by a body corporate that is a  
16 related body corporate of an Australian body corporate  
17 that holds a benchmark administrator licence; and
- 18 (ii) is critical to the administration of a significant financial  
19 benchmark, in accordance with subsection (4);
- 20 (g) an asset that:
- 21 (i) is owned or operated by an Australian body corporate  
22 that holds an Australian derivative trade repository  
23 licence; and
- 24 (ii) is critical to the operation of a derivative trade  
25 repository, in accordance with subsection (5);
- 26 (h) an asset that:
- 27 (i) is owned or operated by a body corporate that is a  
28 related body corporate of an Australian body corporate  
29 that holds an Australian derivative trade repository  
30 licence; and
- 31 (ii) is critical to the operation of a derivative trade  
32 repository, in accordance with subsection (5);
- 33 (i) an asset that is critical to the operation of a payment system,  
34 in accordance with subsection (6).

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



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (2) For the purposes of paragraphs (1)(a) and (b), the rules may  
2 prescribe:  
3 (a) specified assets that are critical to the operation of a financial  
4 market; or  
5 (b) requirements for an asset to be critical to the operation of a  
6 financial market.
- 7 (3) For the purposes of paragraphs (1)(c) and (d), the rules may  
8 prescribe:  
9 (a) specified assets that are critical to the operation of a clearing  
10 and settlement facility; or  
11 (b) requirements for an asset to be critical to the operation of a  
12 clearing and settlement facility.
- 13 (4) For the purposes of paragraphs (1)(e) and (f), the rules may  
14 prescribe:  
15 (a) specified assets that are critical to the administration of a  
16 significant financial benchmark; or  
17 (b) requirements for an asset to be critical to the administration  
18 of a significant financial benchmark.
- 19 (5) For the purposes of paragraphs (1)(g) and (h), the rules may  
20 prescribe:  
21 (a) specified assets that are critical to the operation of a  
22 derivative trade repository; or  
23 (b) requirements for an asset to be critical to the operation of a  
24 derivative trade repository.
- 25 (6) For the purposes of paragraph (1)(i), the rules may prescribe:  
26 (a) specified assets that are critical to the operation of a payment  
27 system; or  
28 (b) requirements for an asset to be critical to the operation of a  
29 payment system.
- 30 (7) For the purposes of this section, *Australian body corporate* means  
31 a body corporate that is incorporated in Australia.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 **12E Meaning of *critical broadcasting asset***

- 2 (1) One or more broadcasting transmission assets are a ***critical***  
3 ***broadcasting asset*** if:  
4 (a) the broadcasting transmission assets are:  
5 (i) owned or operated by the same entity; and  
6 (ii) located on a site, that, in accordance with subsection (2),  
7 is a critical transmission site; or  
8 (b) the broadcasting transmission assets are:  
9 (i) owned or operated by the same entity; and  
10 (ii) located on at least 50 different sites.

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

- 13 (2) For the purposes of paragraph (1)(a), the rules may prescribe:  
14 (a) specified sites that are critical transmission sites; or  
15 (b) requirements for sites to be critical transmission sites.

16 **12F Meaning of *critical data storage or processing asset***

- 17 (1) An asset is a ***critical data storage or processing asset*** if:  
18 (a) it is owned or operated by an entity that is a data storage or  
19 processing provider; and  
20 (b) it is used wholly or primarily in connection with a data  
21 storage or processing service that is provided by the entity on  
22 a commercial basis to an end-user that is:  
23 (i) the Commonwealth; or  
24 (ii) a body corporate established by a law of the  
25 Commonwealth; or  
26 (iii) a State; or  
27 (iv) a body corporate established by a law of a State; or  
28 (v) a Territory; or  
29 (vi) a body corporate established by a law of a Territory; and  
30 (c) the entity knows that the asset is used as described in  
31 paragraph (b).

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

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (2) An asset is a ***critical data storage or processing asset*** if:  
2 (a) it is owned or operated by an entity that is a data storage or  
3 processing provider; and  
4 (b) it is used wholly or primarily in connection with a data  
5 storage or processing service that:  
6 (i) is provided by the entity on a commercial basis to an  
7 end-user that is the responsible entity for a critical  
8 infrastructure asset; and  
9 (ii) relates to business critical data; and  
10 (c) the entity knows that the asset is used as described in  
11 paragraph (b).

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

- 14 (3) If:  
15 (a) an entity (the ***first entity***) is the responsible entity for a  
16 critical infrastructure asset; and  
17 (b) the first entity becomes aware that a data storage or  
18 processing service:  
19 (i) is provided by another entity on a commercial basis to  
20 the first entity; and  
21 (ii) relates to business critical data;  
22 the first entity must:  
23 (c) take reasonable steps to inform that other entity that the first  
24 entity has become aware that the data storage or processing  
25 service:  
26 (i) is provided by the other entity on a commercial basis to  
27 the first entity; and  
28 (ii) relates to business critical data; and  
29 (d) do so as soon as practicable after becoming so aware.

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

## 32 **12G Meaning of *critical banking asset***

- 33 (1) An asset is a ***critical banking asset*** if the asset:  
34 (a) is owned or operated by:  
35 (i) an authorised deposit-taking institution; or
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 (ii) a related body corporate of an authorised deposit-taking  
2 institution; and

3 (b) is critical to the carrying on of banking business by the  
4 authorised deposit-taking institution, in accordance with  
5 subsection (2).

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

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

9 (a) specified assets that are critical to the carrying on of banking  
10 business by an authorised deposit-taking institution; or

11 (b) requirements for an asset to be critical to the carrying on of  
12 banking business by an authorised deposit-taking institution.

### 13 **12H Meaning of *critical insurance asset***

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

16 (a) an asset that:

17 (i) is owned or operated by an entity that carries on  
18 insurance business; and

19 (ii) is critical to the carrying on of insurance business, in  
20 accordance with subsection (2);

21 (b) an asset that:

22 (i) is owned or operated by a body corporate that is a  
23 related body corporate of an entity that carries on  
24 insurance business; and

25 (ii) is critical to the carrying on of insurance business, in  
26 accordance with subsection (2);

27 (c) an asset that is:

28 (i) owned or operated by an entity that carries on life  
29 insurance business; and

30 (ii) is critical to the carrying on of life insurance business,  
31 in accordance with subsection (3);

32 (d) an asset that:

33 (i) is owned or operated by a body corporate that is a  
34 related body corporate of an entity that carries on life  
35 insurance business; and

---

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (ii) is critical to the carrying on of life insurance business,  
2 in accordance with subsection (3);
- 3 (e) an asset that is:
- 4 (i) owned or operated by an entity that carries on health  
5 insurance business; and
- 6 (ii) is critical to the carrying on of health insurance  
7 business, in accordance with subsection (4);
- 8 (f) an asset that:
- 9 (i) is owned or operated by a body corporate that is a  
10 related body corporate of an entity that carries on health  
11 insurance business; and
- 12 (ii) is critical to the carrying on of health insurance  
13 business, in accordance with subsection (4).
- 14 Note: The rules may prescribe that a specified critical insurance asset is not  
15 a critical infrastructure asset (see section 9).
- 16 (2) For the purposes of paragraphs (1)(a) and (b), the rules may  
17 prescribe:
- 18 (a) specified assets that are critical to the carrying on of  
19 insurance business; or
- 20 (b) requirements for an asset to be critical to the carrying on of  
21 insurance business.
- 22 (3) For the purposes of paragraphs (1)(c) and (d), the rules may  
23 prescribe:
- 24 (a) specified assets that are critical to the carrying on of life  
25 insurance business; or
- 26 (b) requirements for an asset to be critical to the carrying on of  
27 life insurance business.
- 28 (4) For the purposes of paragraphs (1)(e) and (f), the rules may  
29 prescribe:
- 30 (a) specified assets that are critical to the carrying on of health  
31 insurance business; or
- 32 (b) requirements for an asset to be critical to the carrying on of  
33 health insurance business.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

#### 12J Meaning of *critical superannuation asset*

- (1) An asset is a *critical superannuation asset* if it is critical to the operation of a registrable superannuation entity, in accordance with subsection (2).

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 subsection (1), the rules may prescribe:

- (a) specified assets that are critical to the operation of a registrable superannuation entity; or
- (b) requirements for an asset to be critical to the operation of a registrable superannuation entity.

#### 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) declared by the rules to be a critical supermarket retailer; or
- (ii) declared by the rules to be a critical food wholesaler; or
- (iii) declared by the rules to be a critical grocery wholesaler.

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 subsection (1), if:

- (a) a network is used for the distribution of food or groceries;  
and

- (b) the network is operated under a contract with an entity referred to in paragraph (1)(b);

the network is taken to be operated by that entity.

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 **12L Meaning of *responsible entity***

2 *Critical telecommunications asset*

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

12 *Critical broadcasting asset*

- 13 (2) The responsible entity for a critical broadcasting asset is:  
14 (a) the entity referred to in whichever of  
15 subparagraphs 12E(1)(a)(i) or (b)(i) is applicable; or  
16 (b) if another entity is prescribed by the rules in relation to the  
17 asset—that other entity.

18 *Critical domain name system*

- 19 (3) The responsible entity for a critical domain name system is:  
20 (a) the entity referred to in paragraph (a) of the definition of  
21 ***critical domain name system*** in section 5; or  
22 (b) if another entity is prescribed by the rules in relation to the  
23 system—that other entity.

24 *Critical data storage or processing asset*

- 25 (4) The responsible entity for a critical data storage or processing asset  
26 is:  
27 (a) the entity referred to in paragraph 12F(1)(a); or  
28 (b) if another entity is prescribed by the rules in relation to the  
29 asset—that other entity.

30 *Critical banking asset*

- 31 (5) The responsible entity for a critical banking asset is:
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (a) the authorised deposit-taking institution referred to in  
2 whichever of subparagraphs 12G(1)(a)(i) or (ii) is applicable;  
3 or  
4 (b) if another entity is prescribed by the rules in relation to the  
5 asset—that other entity.

6 *Critical superannuation asset*

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

12 *Critical insurance asset*

- 13 (7) The responsible entity for a critical insurance asset is:  
14 (a) if the asset is covered by paragraph 12H(1)(a)—the entity  
15 referred to in subparagraph 12H(1)(a)(i); or  
16 (b) if the asset is covered by paragraph 12H(1)(b)—the entity  
17 that carries on insurance business as mentioned in  
18 subparagraph 12H(1)(b)(i); or  
19 (c) if the asset is covered by paragraph 12H(1)(c)—the entity  
20 referred to in subparagraph 12H(1)(c)(i); or  
21 (d) if the asset is covered by paragraph 12H(1)(d)—the entity  
22 that carries on life insurance business as mentioned in  
23 subparagraph 12H(1)(d)(i); or  
24 (e) if the asset is covered by paragraph 12H(1)(e)—the entity  
25 referred to in subparagraph 12H(1)(e)(i); or  
26 (f) if the asset is covered by paragraph 12H(1)(f)—the entity that  
27 carries on health insurance business as mentioned in  
28 subparagraph 12H(1)(f)(i); or  
29 (g) if another entity is prescribed by the rules in relation to the  
30 asset—that other entity.

31 *Critical financial market infrastructure asset*

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



# EXPOSURE DRAFT

- 1 (a) if the asset is covered by paragraph 12D(1)(a)—the body  
2 corporate referred to in subparagraph 12D(1)(a)(i); or  
3 (b) if the asset is covered by paragraph 12D(1)(b)—the body  
4 corporate that holds an Australian market licence as  
5 mentioned in subparagraph 12D(1)(b)(i); or  
6 (c) if the asset is covered by paragraph 12D(1)(c)—the body  
7 corporate referred to in subparagraph 12D(1)(c)(i); or  
8 (d) if the asset is covered by paragraph 12D(1)(d)—the body  
9 corporate that holds an Australian CS facility licence as  
10 mentioned in subparagraph 12D(1)(d)(i); or  
11 (e) if the asset is covered by paragraph 12D(1)(e)—the body  
12 corporate referred to in subparagraph 12D(1)(e)(i); or  
13 (f) if the asset is covered by paragraph 12D(1)(f)—the body  
14 corporate that holds a benchmark administrator licence as  
15 mentioned in subparagraph 12D(1)(f)(i); or  
16 (g) if the asset is covered by paragraph 12D(1)(g)—the body  
17 corporate referred to in subparagraph 12D(1)(g)(i); or  
18 (h) if the asset is covered by paragraph 12D(1)(h)—the body  
19 corporate that holds an Australian derivative trade repository  
20 licence as mentioned in subparagraph 12D(1)(h)(i); or  
21 (i) if the asset is covered by paragraph 12D(1)(i)—the entity  
22 prescribed by the rules; or  
23 (j) if another entity is prescribed by the rules in relation to the  
24 asset—that other entity.

25 *Critical water asset*

- 26 (9) The responsible entity for a critical water asset is:  
27 (a) the water utility that holds the licence, approval or  
28 authorisation (however described), under a law of the  
29 Commonwealth, a State or a Territory, to provide the service  
30 to be delivered by the asset; or  
31 (b) if another entity is prescribed by the rules in relation to the  
32 asset—that other entity.

33 *Critical electricity asset*

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

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

6 *Critical gas asset*

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

13 *Critical energy market operator asset*

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

25 *Critical liquid fuel asset*

- 26 (13) The responsible entity for a critical liquid fuel asset is:  
27 (a) if the asset is a liquid fuel refinery—the entity that operates  
28 the liquid fuel refinery; or  
29 (b) if the asset is a liquid fuel pipeline—the entity that operates  
30 the liquid fuel pipeline; or  
31 (c) if the asset is a liquid fuel storage facility—the entity that  
32 operates the liquid fuel storage facility; or  
33 (d) if another entity is prescribed by the rules in relation to the  
34 asset—that other entity.
-



# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (b) if a State is responsible for the management of the asset—the  
2 State; or  
3 (c) if a Territory is responsible for the management of the  
4 asset—the Territory; or  
5 (d) if a body is:  
6 (i) established by a law of the Commonwealth, a State or a  
7 Territory; and  
8 (ii) responsible for the management of the asset;  
9 that body; or  
10 (e) if none of paragraphs (a), (b), (c), (d) and (e) apply—the  
11 entity prescribed by the rules in relation to the asset; or  
12 (f) if another entity is prescribed by the rules in relation to the  
13 asset—that other entity.

#### 14 *Critical freight services asset*

- 15 (19) The responsible entity for a critical freight services asset is:  
16 (a) the entity referred to in subsection 12C(1); or  
17 (b) if another entity is prescribed by the rules in relation to the  
18 asset—that other entity.

#### 19 *Critical public transport asset*

- 20 (20) The responsible entity for a critical public transport asset is:  
21 (a) the entity referred to in paragraph (a) of the definition of  
22 ***critical public transport asset*** in section 5; or  
23 (b) if another entity is prescribed by the rules in relation to the  
24 asset—that other entity.

#### 25 *Critical aviation asset*

- 26 (21) The responsible entity for a critical aviation asset is:  
27 (a) if the asset is:  
28 (i) used in connection with the provision of an air service;  
29 and  
30 (ii) owned or operated by an aircraft operator;  
31 the aircraft operator; or  
32 (b) if the asset is:
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (i) used in connection with the provision of an air service;  
2 and  
3 (ii) owned or operated by a regulated air cargo agent;  
4 the regulated air cargo agent; or  
5 (c) if the asset is used by an airport operator in connection with  
6 the operation of an airport—the airport operator; or  
7 (d) if another entity is prescribed by the rules in relation to the  
8 asset—that other entity.

9 *Critical defence industry asset*

- 10 (22) The responsible entity for a critical defence industry asset is:  
11 (a) the entity referred to in paragraph (a) of the definition of  
12 *critical defence industry asset*; or  
13 (b) if another entity is prescribed by the rules in relation to the  
14 asset—that other entity.

15 *Assets prescribed by the rules*

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

19 *Assets declared to be a critical infrastructure asset*

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

24 *System of national significance*

- 25 (25) If a critical infrastructure asset is a system of national significance,  
26 the responsible entity for the system of national significance is the  
27 responsible entity for the asset.

28 **12M Meaning of cyber security incident**

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

- 31 (a) unauthorised access to:
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (i) computer data; or  
2 (ii) a computer program;  
3 (b) unauthorised modification of:  
4 (i) computer data; or  
5 (ii) a computer program;  
6 (c) unauthorised impairment of electronic communication to or  
7 from a computer;  
8 (d) unauthorised impairment of the availability, reliability,  
9 security or operation of:  
10 (i) a computer; or  
11 (ii) computer data; or  
12 (iii) a computer program.

### 13 **12N Meaning of unauthorised access, modification or impairment**

- 14 (1) For the purposes of this Act:  
15 (a) access to:  
16 (i) computer data; or  
17 (ii) a computer program; or  
18 (b) modification of:  
19 (i) computer data; or  
20 (ii) a computer program; or  
21 (c) the impairment of electronic communication to or from a  
22 computer; or  
23 (d) the impairment of the availability, reliability, security or  
24 operation of:  
25 (i) a computer; or  
26 (ii) computer data; or  
27 (iii) a computer program;  
28 by a person is unauthorised if the person is not entitled to cause  
29 that access, modification or impairment.
- 30 (2) For the purposes of subsection (1), it is immaterial whether the  
31 person can be identified.
- 32 (3) For the purposes of subsection (1), if:  
33 (a) a person causes any access, modification or impairment of a  
34 kind mentioned in that subsection; and
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (b) the person does so:  
2 (i) under a warrant issued under a law of the  
3 Commonwealth, a State or a Territory; or  
4 (ii) under an emergency authorisation given to the person  
5 under Part 3 of the *Surveillance Devices Act 2004* or  
6 under a law of a State or Territory that makes provision  
7 to similar effect; or  
8 (iii) under a tracking device authorisation given to the  
9 person under section 39 of the *Surveillance Devices Act*  
10 *2004*; or  
11 (iv) in accordance with a technical assistance request; or  
12 (v) in compliance with a technical assistance notice; or  
13 (vi) in compliance with a technical capability notice;  
14 the person is entitled to cause that access, modification or  
15 impairment.

## 16 **12P Examples of responding to a cyber security incident**

- 17 The following are examples of responding to a cyber security  
18 incident:  
19 (a) if the incident is imminent—preventing the incident;  
20 (b) mitigating a relevant impact of the incident on:  
21 (i) a critical infrastructure asset; or  
22 (ii) a critical infrastructure sector asset;  
23 (c) if a critical infrastructure asset or a critical infrastructure  
24 sector asset has been, or is being, affected by the incident—  
25 restoring the functionality of the asset.

## 26 **33 Paragraph 13(1)(b)**

27 Omit “that is a reporting entity for,”, insert “, so far as the entity is a  
28 reporting entity for, a relevant entity for,”.

## 29 **34 At the end of paragraph 13(1)(b)**

- 30 Add:  
31 or (iv) used in the course of, or in relation to, banking to which  
32 paragraph 51(xiii) of the Constitution applies; or  
33 (v) used in the course of, or in relation to, insurance to  
34 which paragraph 51(xiv) of the Constitution applies; or
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (vi) used to supply a carriage service; or  
2 (vii) used in connection with the provision of a broadcasting  
3 service; or  
4 (viii) used to administer a domain name system;

#### 35 Subsection 13(2)

- 5 Omit “also applies”, substitute “and section 60AA (acquisition of  
6 property) also apply”.

#### 36 Division 1 of Part 2 (heading)

- 8 Omit “Simplified outline of this Part”, substitute “Introduction”.

#### 37 At the end of section 18

10 Add:

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

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

13 Add:

#### 18A Application of this Part

15 This Part applies to a critical infrastructure asset if:

- 16 (a) the asset is specified in the rules; or  
17 (b) both:  
18 (i) the asset is the subject of a declaration under section 51;  
19 and  
20 (ii) the declaration determines that this Part applies to the  
21 asset; or  
22 (c) immediately before the commencement of this section, the  
23 asset was a critical infrastructure asset (within the meaning of  
24 this Act as in force immediately before that commencement).

25 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
26 *2003*.

#### 39 After Part 2

28 Insert:



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 **Part 2A—Critical infrastructure risk management**  
2 **programs**  
3

4 **30AA Simplified outline of this Part**

- 5
- 6 • The responsible entity for one or more critical infrastructure  
7 assets must have, and comply with, a critical infrastructure  
8 risk management program.
  - 9 • The purpose of a critical infrastructure risk management  
10 program is to do the following for each of those assets:  
11 (a) identify each hazard where there is a material risk that  
12 the occurrence of the hazard could have a relevant  
13 impact on the asset;  
14 (b) so far as it is reasonably possible to do so—minimise or  
15 eliminate any material risk of such a hazard occurring;  
16 (c) mitigate the relevant impact of such a hazard on the  
17 asset.
  - 18 • A responsible entity must give an annual report relating to its  
19 critical infrastructure risk management program. If the entity  
20 has a board, council or other governing body, the annual  
21 report must be signed by each member of the board, council or  
22 other governing body.

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

23 **30AB Application of this Part**

24 This Part applies to a critical infrastructure asset if:

- 25 (a) the asset is specified in the rules; or  
26 (b) both:  
27 (i) the asset is the subject of a declaration under section 51;  
28 and  
29 (ii) the declaration determines that this Part applies to the  
30 asset.

31 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
32 *2003*.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1     **30AC Responsible entity must have a critical infrastructure risk**  
2             **management program**

3             If an entity is the responsible entity for one or more critical  
4             infrastructure assets, the entity must:

- 5                 (a) adopt; and  
6                 (b) maintain;

7             a critical infrastructure risk management program that applies to  
8             the entity.

9             Civil penalty:         200 penalty units.

10    **30AD Compliance with critical infrastructure risk management**  
11             **program**

12             If:

13                 (a) an entity is the responsible entity for one or more critical  
14                 infrastructure assets; and

15                 (b) the entity has adopted a critical infrastructure risk  
16                 management program that applies to the entity;

17             the entity must comply with:

18                 (c) the critical infrastructure risk management program; or

19                 (d) if the program has been varied on one or more occasions—  
20                 the program as varied.

21             Civil penalty:         200 penalty units.

22    **30AE Review of critical infrastructure risk management program**

23             If:

24                 (a) an entity is the responsible entity for one or more critical  
25                 infrastructure assets; and

26                 (b) the entity has adopted a critical infrastructure risk  
27                 management program that applies to the entity;

28             the entity must review the program on a regular basis.

29             Civil penalty:         200 penalty units.

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

## 1 **30AF Update of critical infrastructure risk management program**

2 If:

3 (a) an entity is the responsible entity for one or more critical  
4 infrastructure assets; and

5 (b) the entity has adopted a critical infrastructure risk  
6 management program that applies to the entity;

7 the entity must take all reasonable steps to ensure that the program  
8 is up to date.

9 Civil penalty: 200 penalty units.

## 10 **30AG Responsible entity must submit annual report**

11 *Scope*

12 (1) This section applies if, during a period (the *relevant period*) that  
13 consists of the whole or a part of a financial year:

14 (a) an entity was the responsible entity for one or more critical  
15 infrastructure assets; and

16 (b) the entity had a critical infrastructure risk management  
17 program that applied to the entity.

18 *Annual report*

19 (2) The entity must, within 30 days after the end of the financial year,  
20 give:

21 (a) if there is a relevant Commonwealth regulator that has  
22 functions relating to the security of those assets—the relevant  
23 Commonwealth regulator; or

24 (b) in any other case—the Secretary;

25 a report that:

26 (c) if the entity had the program at the end of the financial  
27 year—includes whichever of the following statements is  
28 applicable:

29 (i) if the program was up to date at the end of the financial  
30 year—a statement to that effect;

31 (ii) if the program was not up to date at the end of the  
32 financial year—a statement to that effect; and

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (d) if a hazard had a significant relevant impact on one or more  
2 of those assets during the relevant period—includes a  
3 statement that:  
4 (i) identifies the hazard; and  
5 (ii) evaluates the effectiveness of the program in mitigating  
6 the significant relevant impact of the hazard on the  
7 assets concerned; and  
8 (iii) if the program was varied during the financial year as a  
9 result of the occurrence of the hazard—outlines the  
10 variation; and  
11 (e) is in the approved form; and  
12 (f) if the entity has a board, council or other governing body—is  
13 signed by each member of the board, council or other  
14 governing body, as the case requires.

15 Civil penalty: 150 penalty units.

- 16 (3) A report given by an entity under subsection (2) is not admissible  
17 in evidence against the entity in civil proceedings relating to a  
18 contravention of a civil penalty provision of this Act.

### 19 **30AH Critical infrastructure risk management program**

- 20 (1) A *critical infrastructure risk management program* is a written  
21 program:  
22 (a) that applies to a particular entity that is the responsible entity  
23 for one or more critical infrastructure assets; and  
24 (b) the purpose of which is to do the following for each of those  
25 assets:  
26 (i) identify each hazard where there is a material risk that  
27 the occurrence of the hazard could have a relevant  
28 impact on the asset;  
29 (ii) so far as it is reasonably possible to do so—minimise or  
30 eliminate any material risk of such a hazard occurring;  
31 (iii) mitigate the relevant impact of such a hazard on the  
32 asset; and  
33 (c) that complies with such requirements (if any) as are specified  
34 in the rules.

- 35 (2) Requirements specified under paragraph (1)(c):
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (a) may be of general application; or  
2 (b) may relate to one or more specified critical infrastructure  
3 assets.
- 4 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
5 *2003*.
- 6 (3) Subsection (2) of this section does not, by implication, limit  
7 subsection 33(3A) of the *Acts Interpretation Act 1901*.
- 8 (4) Rules made for the purposes of paragraph (1)(c) may require that a  
9 critical infrastructure risk management program include provisions  
10 that require background checks of individuals to be conducted  
11 under the AusCheck scheme.
- 12 (5) Subsection (4) does not limit paragraph (1)(c).
- 13 (6) For the purposes of this section, in determining whether a risk is a  
14 material risk, regard must be had to:  
15 (a) the likelihood of the hazard occurring; and  
16 (b) the relevant impact of the hazard on the asset if the hazard  
17 were to occur.
- 18 (7) The rules may provide that a specified risk is taken to be a material  
19 risk for the purposes of this section.
- 20 (8) The rules may provide that the taking of specified action in relation  
21 to a critical infrastructure asset is taken to be action that minimises  
22 or eliminates any material risk that the occurrence of a specified  
23 hazard could have a relevant impact on the asset.
- 24 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
25 *2003*.
- 26 (9) The rules may provide that the taking of specified action in relation  
27 to a specified critical infrastructure asset is taken to be action that  
28 minimises or eliminates any material risk that the occurrence of a  
29 specified hazard could have a relevant impact on the asset.
- 30 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
31 *2003*.
- 32 (10) The rules may provide that the taking of specified action in relation  
33 to a critical infrastructure asset is taken to be action that mitigates  
34 the relevant impact of a specified hazard on the asset.
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
2 2003.

3 (11) The rules may provide that the taking of specified action in relation  
4 to a specified critical infrastructure asset is taken to be action that  
5 mitigates the relevant impact of a specified hazard on the asset.

6 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
7 2003.

#### 8 **30AJ Variation of critical infrastructure risk management program**

9 A critical infrastructure risk management program may be varied,  
10 so long as the varied program is a critical infrastructure risk  
11 management program.

#### 12 **30AK Revocation of adoption of critical infrastructure risk** 13 **management program**

14 If an entity has adopted a critical infrastructure risk management  
15 program that applies to the entity, this Part does not prevent the  
16 entity from:

- 17 (a) revoking that adoption; and  
18 (b) adopting another critical infrastructure risk management  
19 program that applies to the entity.

#### 20 **30AL Consultation—rules**

##### 21 *Scope*

22 (1) This section applies to rules made for the purposes of  
23 section 30AH.

##### 24 *Consultation*

25 (2) Before making or amending the rules, the Minister must:

- 26 (a) cause to be published on the Department's website a notice:  
27 (i) setting out the draft rules or amendments; and  
28 (ii) inviting persons to make submissions to the Minister  
29 about the draft rules or amendments within 14 days after  
30 the notice is published; and  
31 (b) give a copy of the notice to each First Minister; and
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 (c) consider any submissions received within the 14-day period  
2 mentioned in paragraph (a).

3 (3) Subsection (2) does not apply if:

4 (a) the Minister is satisfied that there is an imminent threat that a  
5 hazard will have a significant relevant impact on a critical  
6 infrastructure asset; or

7 (b) the Minister is satisfied that a hazard has had, or is having, a  
8 significant relevant impact on a critical infrastructure asset.

9 Note: See also section 30AM (review of rules).

## 10 **30AM Review of rules**

### 11 *Scope*

12 (1) This section applies if, because of subsection 30AL(3),  
13 subsection 30AL(2) did not apply to the making of:

14 (a) rules; or

15 (b) amendments.

### 16 *Review of rules*

17 (2) The Secretary must:

18 (a) if paragraph (1)(a) applies—review the operation,  
19 effectiveness and implications of the rules; and

20 (b) if paragraph (1)(b) applies—review the operation,  
21 effectiveness and implications of the amendments; and

22 (c) without limiting paragraph (a) or (b), consider whether any  
23 amendments should be made; and

24 (d) give the Minister:

25 (i) a report of the review; and

26 (ii) a statement setting out the Secretary's findings.

27 (3) For the purposes of the review, the Secretary must:

28 (a) cause to be published on the Department's website a notice:

29 (i) setting out the rules or amendments concerned; and

30 (ii) inviting persons to make submissions to the Secretary  
31 about the rules or amendments concerned within 14  
32 days after the notice is published; and

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 (b) consider any submissions received within the 14-day period  
2 mentioned in paragraph (a).

3 (4) The Secretary must complete the review within 60 days after the  
4 commencement of the rules or amendments concerned.

5 *Minister to table statement of findings*

6 (5) The Minister must cause a copy of the statement of findings to be  
7 tabled in each House of the Parliament within 15 sitting days of  
8 that House after the Minister receives it.

9 **30AN Application, adoption or incorporation of a law of a State or**  
10 **Territory etc.**

11 *Scope*

12 (1) This section applies to rules made for the purposes of  
13 section 30AH.

14 *Application, adoption or incorporation of a law of a State or*  
15 *Territory*

16 (2) Despite subsection 14(2) of the *Legislation Act 2003*, the rules may  
17 make provision in relation to a matter by applying, adopting or  
18 incorporating, with or without modification, any matter contained  
19 in a law of a State or Territory as in force or existing from time to  
20 time.

21 *Application, adoption or incorporation of a standard*

22 (3) Despite subsection 14(2) of the *Legislation Act 2003*, the rules may  
23 make provision in relation to a matter by applying, adopting or  
24 incorporating, with or without modification, any matter contained  
25 in a standard proposed or approved by Standards Australia as in  
26 force or existing from time to time.

27 Note: The expression *Standards Australia* is defined in section 2B of the  
28 *Acts Interpretation Act 1901*.



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 **Part 2B—Notification of cyber security incidents**  
2

3 **30BA Simplified outline of this Part**

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

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

9 **30BB Application of this Part**

10 This Part applies to a critical infrastructure asset if:

- 11 (a) the asset is specified in the rules; or  
12 (b) both:  
13 (i) the asset is the subject of a declaration under section 51;  
14 and  
15 (ii) the declaration determines that this Part applies to the  
16 asset.

17 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
18 *2003*.

19 **30BC Notification of critical cyber security incidents**

- 20 (1) If:  
21 (a) an entity is the responsible entity for a critical infrastructure  
22 asset; and  
23 (b) the entity becomes aware that:  
24 (i) a cyber security incident has occurred or is occurring;  
25 and  
26 (ii) the incident has had, or is having, a significant impact  
27 (whether direct or indirect) on the availability of the  
28 asset;  
29 the entity must:  
30 (c) give the relevant Commonwealth body (see section 30BF) a  
31 report that:

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (i) is about the incident; and  
2 (ii) includes such information (if any) as is prescribed by  
3 the rules; and  
4 (d) do so as soon as practicable, and in any event within 12  
5 hours, after the entity becomes so aware.
- 6 Civil penalty: 50 penalty units.
- 7 *Form of report etc.*
- 8 (2) A report under subsection (1) may be given:  
9 (a) orally; or  
10 (b) in writing.
- 11 (3) If a report under subsection (1) is given orally, the entity must:  
12 (a) do both of the following:  
13 (i) make a written record of the report in the approved  
14 form;  
15 (ii) give a copy of the written record of the report to the  
16 relevant Commonwealth body (see section 30BF); and  
17 (b) do so within 48 hours after the report is given.
- 18 Civil penalty: 50 penalty units.
- 19 (4) If the report is given in writing, the entity must ensure that the  
20 report is in the approved form.
- 21 Civil penalty: 50 penalty units.

### 30BD Notification of other cyber security incidents

- 22 (1) If:  
23 (a) an entity is the responsible entity for a critical infrastructure  
24 asset; and  
25 (b) the entity becomes aware that:  
26 (i) a cyber security incident has occurred, is occurring or is  
27 imminent; and  
28 (ii) the incident has had, is having, or is likely to have, a  
29 relevant impact on the asset;  
30 the entity must:  
31

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (c) give the relevant Commonwealth body (see section 30BF) a  
2 report that:  
3 (i) is about the incident; and  
4 (ii) includes such information (if any) as is prescribed by  
5 the rules; and  
6 (d) do so as soon as practicable, and in any event within 24  
7 hours, after the entity becomes so aware.

8 Civil penalty: 50 penalty units.

9 *Form of report etc.*

- 10 (2) A report under subsection (1) may be given:  
11 (a) orally; or  
12 (b) in writing.
- 13 (3) If a report under subsection (1) is given orally, the entity must:  
14 (a) do both of the following:  
15 (i) make a written record of the report in the approved  
16 form;  
17 (ii) give a copy of the written record of the report to the  
18 relevant Commonwealth body (see section 30BF); and  
19 (b) do so within 48 hours after the report is given.

20 Civil penalty: 50 penalty units.

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

23 Civil penalty: 50 penalty units.

## 24 **30BE Liability**

- 25 (1) An entity is not liable to an action or other proceeding for damages  
26 for or in relation to an act done or omitted in good faith in  
27 compliance with section 30BC or section 30BD.
- 28 (2) An officer, employee or agent of an entity is not liable to an action  
29 or other proceeding for damages for or in relation to an act done or  
30 omitted in good faith in connection with an act done or omitted by  
31 the entity as mentioned in subsection (1).

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 **30BF Relevant Commonwealth body**

2 For the purposes of this Part, *relevant Commonwealth body*  
3 means:

- 4 (a) a Department that is specified in the rules; or  
5 (b) a body that is:  
6 (i) established by a law of the Commonwealth; and  
7 (ii) specified in the rules; or  
8 (c) if:  
9 (i) no rules are in force for the purposes of paragraph (a);  
10 and  
11 (ii) no rules are in force for the purposes of paragraph (b);  
12 ASD.

13 **Part 2C—Enhanced cyber security obligations**

14 **Division 1—Simplified outline of this Part**

15 **30CA Simplified outline of this Part**

- 16 • This Part sets out enhanced cyber security obligations that  
17 relate to systems of national significance.
- 18 • The responsible entity for a system of national significance  
19 may be subject to statutory incident response planning  
20 obligations.
- 21 • The responsible entity for a system of national significance  
22 may be required to undertake a cyber security exercise.
- 23 • The responsible entity for a system of national significance  
24 may be required to undertake a vulnerability assessment.
- 25 • If a computer is a system of national significance, or is needed  
26 to operate a system of national significance, the responsible  
27 entity for the system may be required to:  
28 (a) give ASD periodic reports of system information; or  
29 (b) give ASD event-based reports of system information; or
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 (c) install software that transmits system information to  
2 ASD.

3 Note: For declaration of a system of national significance, see section 52B.

## 4 **Division 2—Statutory incident response planning** 5 **obligations**

### 6 **Subdivision A—Application of statutory incident response** 7 **planning obligations**

#### 8 **30CB Application of statutory incident response planning** 9 **obligations—determination by the Secretary**

- 10 (1) The Secretary may, by written notice given to an entity that is the  
11 responsible entity for a system of national significance, determine  
12 that the statutory incident response planning obligations apply to  
13 the entity in relation to:
- 14 (a) the system; and
  - 15 (b) cyber security incidents.
- 16 (2) A determination under this section takes effect at the time specified  
17 in the determination.
- 18 (3) The specified time must not be earlier than the end of the 30-day  
19 period that began when the notice was given.
- 20 (4) A determination under this section is not a legislative instrument.

#### 21 **30CC Revocation of determination**

##### 22 *Scope*

- 23 (1) This section applies if:
- 24 (a) a determination is in force under section 30CB; and
  - 25 (b) notice of the determination was given to a particular entity.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1                                    *Power to revoke determination*

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

4                                    *Application of Acts Interpretation Act 1901*

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

### 9                                    **Subdivision B—Statutory incident response planning** 10                                    **obligations**

#### 11                                    **30CD Responsible entity must have an incident response plan**

12                                    If:

- 13                                    (a) an entity is the responsible entity for a system of national  
14                                    significance; and  
15                                    (b) the statutory incident response planning obligations apply to  
16                                    the entity in relation to:  
17                                    (i) the system; and  
18                                    (ii) cyber security incidents;

19                                    the entity must:

- 20                                    (c) adopt; and  
21                                    (d) maintain;  
22                                    an incident response plan that applies to the entity in relation to:  
23                                    (e) the system; and  
24                                    (f) cyber security incidents.

25                                    Civil penalty:            200 penalty units.

#### 26                                    **30CE Compliance with incident response plan**

27                                    If:

- 28                                    (a) an entity is the responsible entity for a system of national  
29                                    significance; and

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (b) the entity has adopted an incident response plan that applies  
2 to the entity;  
3 the entity must comply with:  
4 (c) the incident response plan; or  
5 (d) if the plan has been varied on one or more occasions—the  
6 plan as varied.  
7 Civil penalty: 200 penalty units.

## 8 **30CF Review of incident response plan**

- 9 If:  
10 (a) an entity is the responsible entity for a system of national  
11 significance; and  
12 (b) the entity has adopted an incident response plan that applies  
13 to the entity;  
14 the entity must review the plan on a regular basis.  
15 Civil penalty: 200 penalty units.

## 16 **30CG Update of incident response plan**

- 17 If:  
18 (a) an entity is the responsible entity for a system of national  
19 significance; and  
20 (b) the entity has adopted an incident response plan that applies  
21 to the entity;  
22 the entity must take all reasonable steps to ensure that the plan is  
23 up to date.  
24 Civil penalty: 200 penalty units.

## 25 **30CH Copy of incident response plan must be given to the Secretary**

- 26 (1) If:  
27 (a) an entity is the responsible entity for a system of national  
28 significance; and  
29 (b) the entity adopts an incident response plan that applies to the  
30 entity;  
31 the entity must:
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (c) provide a copy of the incident response plan to the Secretary;  
2 and  
3 (d) do so as soon as practicable after the adoption.

4 Civil penalty: 200 penalty units.

5 (2) If:

- 6 (a) an entity is the responsible entity for a system of national  
7 significance; and  
8 (b) the entity varies an incident response plan that applies to the  
9 entity;  
10 the entity must:  
11 (c) provide a copy of the varied incident response plan to the  
12 Secretary; and  
13 (d) do so as soon as practicable after the variation.

14 Civil penalty: 200 penalty units.

### 15 **30CJ Incident response plan**

16 (1) An *incident response plan* is a written plan:

- 17 (a) that applies to an entity that is the responsible entity for a  
18 system of national significance; and  
19 (b) that relates to the system; and  
20 (c) that relates to cyber security incidents; and  
21 (d) the purpose of which is to plan for responding to cyber  
22 security incidents that could have a relevant impact on the  
23 system; and  
24 (e) that complies with such requirements (if any) as are specified  
25 in the rules.

26 (2) Requirements specified under paragraph (1)(e):

- 27 (a) may be of general application; or  
28 (b) may relate to one or more specified systems of national  
29 significance; or  
30 (c) may relate to one or more specified types of cyber security  
31 incidents.

32 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
33 *2003*.



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (3) Subsection (2) of this section does not, by implication, limit  
2 subsection 33(3A) of the *Acts Interpretation Act 1901*.

## 3 30CK Variation of incident response plan

4 An incident response plan may be varied, so long as the varied plan  
5 is an incident response plan.

## 6 30CL Revocation of adoption of incident response plan

7 If an entity has adopted an incident response plan that applies to  
8 the entity, this Division does not prevent the entity from:

- 9 (a) revoking that adoption; and  
10 (b) adopting another incident response plan that applies to the  
11 entity.

## 12 Division 3—Cyber security exercises

### 13 30CM Requirement to undertake cyber security exercise

14 (1) The Secretary may, by written notice given to an entity that is the  
15 responsible entity for a system of national significance, require the  
16 entity to:

- 17 (a) undertake a cyber security exercise in relation to:  
18 (i) the system; and  
19 (ii) all types of cyber security incidents; and  
20 (b) do so within the period specified in the notice.

21 (2) The Secretary may, by written notice given to an entity that is the  
22 responsible entity for a system of national significance, require the  
23 entity to:

- 24 (a) undertake a cyber security exercise in relation to:  
25 (i) the system; and  
26 (ii) one or more specified types of cyber security incidents;  
27 and  
28 (b) do so within the period specified in the notice.

29 (3) The period specified in a notice under subsection (1) or (2) must  
30 not be earlier than the end of the 30-day period that began when  
31 the notice was given.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (4) A notice under subsection (1) or (2) may also require the entity to  
2 do any or all of the following things:
- 3 (a) allow one or more specified designated officers to observe  
4 the cyber security exercise;
- 5 (b) provide those designated officers with access to premises for  
6 the purposes of observing the cyber security exercise;
- 7 (c) provide those designated officers with reasonable assistance  
8 and facilities that are reasonably necessary to allow those  
9 designated officers to observe the cyber security exercise;
- 10 (d) allow those designated officers to make such records as are  
11 reasonably necessary for the purposes of monitoring  
12 compliance with the notice;
- 13 (e) give those designated officers reasonable notice of the time  
14 when the cyber security exercise will begin.

### 15 **30CN Cyber security exercise**

- 16 (1) A *cyber security exercise* is an exercise:
- 17 (a) that is undertaken by the responsible entity for a system of  
18 national significance; and
- 19 (b) that relates to the system; and
- 20 (c) that either:
- 21 (i) relates to all types of cyber security incidents; or
- 22 (ii) relates to one or more specified types of cyber security  
23 incidents; and
- 24 (d) if the exercise relates to all types of cyber security  
25 incidents—the purpose of which is to:
- 26 (i) test the entity’s ability to respond appropriately to all  
27 types of cyber security incidents that could have a  
28 relevant impact on the system; and
- 29 (ii) test the entity’s preparedness to respond appropriately to  
30 all types of cyber security incidents that could have a  
31 relevant impact on the system; and
- 32 (iii) test the entity’s ability to mitigate the relevant impacts  
33 that all types of cyber security incidents could have on  
34 the system; and
- 35 (e) if the exercise relates to one or more specified types of cyber  
36 security incidents—the purpose of which is to:
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (i) test the entity's ability to respond appropriately to those  
2 types of cyber security incidents that could have a  
3 relevant impact on the system; and  
4 (ii) test the entity's preparedness to respond appropriately to  
5 those types of cyber security incidents that could have a  
6 relevant impact on the system; and  
7 (iii) test the entity's ability to mitigate the relevant impacts  
8 that those types of cyber security incidents could have  
9 on the system; and  
10 (f) that complies with such requirements (if any) as are specified  
11 in the rules.

- 12 (2) Requirements specified under paragraph (1)(f):  
13 (a) may be of general application; or  
14 (b) may relate to one or more specified systems of national  
15 significance; or  
16 (c) may relate to one or more specified types of cyber security  
17 incidents.

18 Note: For specification by class, see subsection 13(3) of the *Legislation Act*  
19 *2003*.

- 20 (3) Subsection (2) of this section does not, by implication, limit  
21 subsection 33(3A) of the *Acts Interpretation Act 1901*.

## 22 **30CP Compliance with requirement to undertake cyber security** 23 **exercise**

24 An entity must comply with a notice given to the entity under  
25 section 30CM.

26 Civil penalty: 200 penalty units.

## 27 **30CQ Internal evaluation report**

- 28 (1) If an entity undertakes a cyber security exercise under  
29 section 30CM, the entity must:  
30 (a) do both of the following:  
31 (i) prepare an evaluation report relating to the cyber  
32 security exercise;  
33 (ii) give a copy of the report to the Secretary; and
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (b) do so:
- 2 (i) within 30 days after the completion of the exercise; or
- 3 (ii) if the Secretary allows a longer period—within that
- 4 longer period.
- 5 Civil penalty: 200 penalty units.
- 6 (2) An evaluation report prepared by an entity under subsection (1) is
- 7 not admissible in evidence against the entity in civil proceedings
- 8 relating to a contravention of a civil penalty provision of this Act
- 9 (other than subsection (1)).

### 10 **30CR External evaluation report**

#### 11 *Scope*

- 12 (1) This section applies if an entity has undertaken a cyber security
- 13 exercise under section 30CM, and:
- 14 (a) all of the following conditions are satisfied:
- 15 (i) the entity has prepared, or purported to prepare, an
- 16 evaluation report under section 30CQ relating to the
- 17 exercise;
- 18 (ii) the entity has given a copy of the report to the
- 19 Secretary;
- 20 (iii) the Secretary has reasonable grounds to believe that the
- 21 report was not prepared appropriately; or
- 22 (b) the entity has contravened section 30CQ.

#### 23 *Requirement*

- 24 (2) The Secretary may, by written notice given to the entity, require
- 25 the entity to:
- 26 (a) appoint an external auditor; and
- 27 (b) arrange for the external auditor to prepare an evaluation
- 28 report (the *new evaluation report*) relating to the exercise;
- 29 and
- 30 (c) arrange for the external auditor to give the new evaluation
- 31 report to the entity; and
- 32 (d) give the Secretary a copy of the new evaluation report within:
- 33 (i) the period specified in the notice; or

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 (ii) if the Secretary allows a longer period—that longer  
2 period.

3 (3) The notice must specify:

- 4 (a) the matters to be covered by the new evaluation report; and  
5 (b) the form of the new evaluation report and the kinds of details  
6 it is to contain.

7 *Eligibility for appointment as an external auditor*

8 (4) An individual is not eligible to be appointed an external auditor by  
9 the entity if the individual is an officer, employee or agent of the  
10 entity.

11 *Compliance*

12 (5) An entity must comply with a requirement under subsection (2).

13 Civil penalty: 200 penalty units.

14 *Immunity*

15 (6) The new evaluation report is not admissible in evidence against the  
16 entity in civil proceedings relating to a contravention of a civil  
17 penalty provision of this Act (other than subsection (5)).

## 18 **30CS Meaning of evaluation report**

19 An *evaluation report*, in relation to a cyber security exercise that  
20 was undertaken in relation to a system of national significance, is a  
21 written report:

- 22 (a) if the exercise relates to all types of cyber security  
23 incidents—the purpose of which is to:  
24 (i) evaluate the entity’s ability to respond appropriately to  
25 all types of cyber security incidents that could have a  
26 relevant impact on the system; and  
27 (ii) evaluate the entity’s preparedness to respond  
28 appropriately to all types of cyber security incidents that  
29 could have a relevant impact on the system; and

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (iii) evaluate the entity's ability to mitigate the relevant  
2 impacts that all types of cyber security incidents could  
3 have on the system; and
- 4 (b) if the exercise relates to one or more specified types of cyber  
5 security incidents—the purpose of which is to:
- 6 (i) evaluate the entity's ability to respond appropriately to  
7 those types of cyber security incidents that could have a  
8 relevant impact on the system; and
- 9 (ii) evaluate the entity's preparedness to respond  
10 appropriately to those types of cyber security incidents  
11 that could have a relevant impact on the system; and
- 12 (iii) evaluate the entity's ability to mitigate the relevant  
13 impacts that those types of cyber security incidents  
14 could have on the system; and
- 15 (c) that complies with such requirements (if any) as are specified  
16 in the rules.

### 17 **30CT External auditors**

- 18 (1) The Secretary may, by writing, authorise a specified individual to  
19 be an external auditor for the purposes of this Act.

20 Note: For specification by class, see subsection 33(3AB) of the *Acts*  
21 *Interpretation Act 1901*.

- 22 (2) An authorisation under subsection (1) is not a legislative  
23 instrument.

### 24 **Division 4—Vulnerability assessments**

#### 25 **30CU Requirement to undertake vulnerability assessment**

- 26 (1) The Secretary may, by written notice given to an entity that is the  
27 responsible entity for a system of national significance, require the  
28 entity to:
- 29 (a) undertake, or cause to be undertaken, a vulnerability  
30 assessment in relation to:
- 31 (i) the system; and  
32 (ii) all types of cyber security incidents; and  
33 (b) do so within the period specified in the notice.

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (2) The Secretary may, by written notice given to an entity that is the  
2 responsible entity for a system of national significance, require the  
3 entity to:
- 4 (a) undertake, or cause to be undertaken, a vulnerability  
5 assessment in relation to:
- 6 (i) the system; and  
7 (ii) one or more specified types of cyber security incidents;  
8 and  
9 (b) do so within the period specified in the notice.
- 10 (3) Before giving a notice to an entity under this section, the Secretary  
11 must consult the entity.

## 12 **30CV Compliance with requirement to undertake a vulnerability** 13 **assessment**

14 An entity must comply with a notice given to the entity under  
15 section 30CU.

16 Civil penalty: 200 penalty units.

## 17 **30CW Designated officers may undertake a vulnerability assessment**

### 18 *Scope*

- 19 (1) This section applies if:
- 20 (a) an entity is the responsible entity for a system of national  
21 significance; and  
22 (b) either:
- 23 (i) the Secretary has reasonable grounds to believe that if  
24 the entity were to be given a notice under  
25 subsection 30CU(1) or (2), the entity would not be  
26 capable of complying with the notice; or  
27 (ii) the entity has not complied with a notice given to the  
28 entity under subsection 30CU(1) or (2).

### 29 *Request*

- 30 (2) The Secretary may give a designated officer a written request to:  
31 (a) undertake a vulnerability assessment in relation to:
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (i) the system; and  
2 (ii) all types of cyber security incidents; and  
3 (b) do so within the period specified in the request.
- 4 (3) The Secretary may give a designated officer a written request to:  
5 (a) undertake a vulnerability assessment in relation to:  
6 (i) the system; and  
7 (ii) one or more specified types of cyber security incidents;  
8 and  
9 (b) do so within the period specified in the request.
- 10 (4) Before giving a request under subsection (2) or (3), the Secretary  
11 must consult the entity.

#### 12 *Requirement*

- 13 (5) If a request under subsection (2) or (3) is given to a designated  
14 officer, the Secretary may, by written notice given to the entity,  
15 require the entity to do any or all of the following things:  
16 (a) provide the designated officer with access to premises for the  
17 purposes of undertaking the vulnerability assessment;  
18 (b) provide the designated officer with access to computers for  
19 the purposes of undertaking the vulnerability assessment;  
20 (c) provide the designated officer with reasonable assistance and  
21 facilities that are reasonably necessary to allow the  
22 designated officer to undertake the vulnerability assessment.

#### 23 *Notification of request*

- 24 (6) If a request under subsection (2) or (3) is given to a designated  
25 officer, the Secretary must give a copy of the request to the entity.

### 26 **30CX Compliance with requirement to provide reasonable** 27 **assistance etc.**

28 An entity must comply with a notice given to the entity under  
29 subsection 30CW(5).

30 Civil penalty: 200 penalty units.

---



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

## 1 **30CY Vulnerability assessment**

- 2 (1) A *vulnerability assessment* is an assessment:
- 3 (a) that relates to a system of national significance; and
- 4 (b) that either:
- 5 (i) relates to all types of cyber security incidents; or
- 6 (ii) relates to one or more specified types of cyber security
- 7 incidents; and
- 8 (c) if the assessment relates to all types of cyber security
- 9 incidents—the purpose of which is to test the vulnerability of
- 10 the system to all types of cyber security incidents; and
- 11 (d) if the assessment relates to one or more specified types of
- 12 cyber security incidents—the purpose of which is to test the
- 13 vulnerability of the system to those types of cyber security
- 14 incidents; and
- 15 (e) that complies with such requirements (if any) as are specified
- 16 in the rules.

- 17 (2) Requirements specified under paragraph (1)(e):
- 18 (a) may be of general application; or
- 19 (b) may relate to one or more specified systems of national
- 20 significance; or
- 21 (c) may relate to one or more specified types of cyber security
- 22 incidents.

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

24 *2003*.

- 25 (3) Subsection (2) of this section does not, by implication, limit
- 26 subsection 33(3A) of the *Acts Interpretation Act 1901*.

## 27 **30CZ Vulnerability assessment report**

- 28 (1) If an entity undertakes a vulnerability assessment under
- 29 section 30CU, the entity must:
- 30 (a) do both of the following:
- 31 (i) prepare, or cause to be prepared, a vulnerability
- 32 assessment report relating to the assessment;
- 33 (ii) give a copy of the report to the Secretary; and
- 34 (b) do so:

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (i) within 30 days after the completion of the assessment;  
2 or  
3 (ii) if the Secretary allows a longer period—within that  
4 longer period.

5 Civil penalty: 200 penalty units.

- 6 (2) If a designated officer undertakes a vulnerability assessment in  
7 accordance with a request given to the designated officer under  
8 section 30CW, the designated officer must:  
9 (a) do both of the following:  
10 (i) prepare a vulnerability assessment report relating to the  
11 assessment;  
12 (ii) give a copy of the report to the Secretary; and  
13 (b) do so:  
14 (i) within 30 days after the completion of the assessment;  
15 or  
16 (ii) if the Secretary allows a longer period—within that  
17 longer period.
- 18 (3) If an entity prepares, or causes to be prepared, a report under  
19 subsection (1), the report is not admissible in evidence against the  
20 entity in civil proceedings relating to a contravention of a civil  
21 penalty provision of this Act (other than subsection (1)).

### 22 **30DA Meaning of vulnerability assessment report**

23 A *vulnerability assessment report*, in relation to a vulnerability  
24 assessment that was undertaken in relation to a system of national  
25 significance, is a written report:

- 26 (a) if the assessment relates to all types of cyber security  
27 incidents—the purpose of which is to assess the vulnerability  
28 of the system to all types of cyber security incidents; and  
29 (b) if the assessment relates to one or more specified types of  
30 cyber security incidents—the purpose of which is to assess  
31 the vulnerability of the system to those types of cyber  
32 security incidents; and  
33 (c) that complies with such requirements (if any) as are specified  
34 in the rules.

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 **Division 5—Access to system information**

2 **Subdivision A—System information reporting notices**

3 **30DB Secretary may require periodic reporting of system**  
4 **information**

5 *Scope*

6 (1) This section applies if:

7 (a) a computer:

8 (i) is needed to operate a system of national significance;  
9 or

10 (ii) is a system of national significance; and

11 (b) the Secretary believes on reasonable grounds that the  
12 responsible entity for the system of national significance is  
13 technically capable of preparing periodic reports consisting  
14 of information that:

15 (i) relates to the operation of the computer; and

16 (ii) may assist with determining whether a power under this  
17 Act should be exercised in relation to the system of  
18 national significance; and

19 (iii) is not personal information (within the meaning of the  
20 *Privacy Act 1988*).

21 *Requirement*

22 (2) The Secretary may, by written notice given to the entity, require  
23 the entity to:

24 (a) prepare periodic reports that:

25 (i) consist of any such information; and

26 (ii) relate to such regular intervals as are specified in the  
27 notice; and

28 (b) prepare those periodic reports:

29 (i) in the manner and form specified in the notice; and

30 (ii) in accordance with the information technology  
31 requirements specified in the notice; and

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 (c) give each of those periodic reports to ASD within the period  
2 ascertained in accordance with the notice in relation to the  
3 periodic report concerned.

4 (3) A notice under subsection (2) is to be known as a *system*  
5 *information periodic reporting notice*.

6 (4) In deciding whether to give a system information periodic  
7 reporting notice to the entity, the Secretary must have regard to:

8 (a) the costs that are likely to be incurred by the entity in  
9 complying with the notice; and

10 (b) such other matters (if any) as the Secretary considers  
11 relevant.

12 *Matters to be set out in notice*

13 (5) A system information periodic reporting notice must set out the  
14 effect of section 30DF.

15 *Other powers not limited*

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

### 18 **30DC Secretary may require event-based reporting of system** 19 **information**

20 *Scope*

21 (1) This section applies if:

22 (a) a computer:

23 (i) is needed to operate a system of national significance;

24 or

25 (ii) is a system of national significance; and

26 (b) the Secretary believes on reasonable grounds that, each time  
27 a particular kind of event occurs, the responsible entity for  
28 the system of national significance will be technically  
29 capable of preparing a report consisting of information that:

30 (i) relates to the operation of the computer; and

---

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (ii) may assist with determining whether a power under this  
2 Act should be exercised in relation to the system of  
3 national significance; and  
4 (iii) is not personal information (within the meaning of the  
5 *Privacy Act 1988*).

6 *Requirement*

- 7 (2) The Secretary may, by written notice given to the entity, require  
8 the entity to do the following things each time an event of that kind  
9 occurs:  
10 (a) prepare a report that consists of any such information;  
11 (b) prepare that report:  
12 (i) in the manner and form specified in the notice; and  
13 (ii) in accordance with the information technology  
14 requirements specified in the notice;  
15 (c) give that report to ASD as soon as practicable after the event  
16 occurs.
- 17 (3) A notice under subsection (2) is to be known as a ***system***  
18 ***information event-based reporting notice***.
- 19 (4) In deciding whether to give a system information event-based  
20 reporting notice to the entity, the Secretary must have regard to:  
21 (a) the costs that are likely to be incurred by the entity in  
22 complying with the notice; and  
23 (b) such other matters (if any) as the Secretary considers  
24 relevant.

25 *Matters to be set out in notice*

- 26 (5) A system information event-based reporting notice must set out the  
27 effect of section 30DF.

28 *Other powers not limited*

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1     **30DD Consultation**

2             Before giving:

- 3                 (a) a system information periodic reporting notice; or  
4                 (b) a system information event-based reporting notice;  
5             to an entity, the Secretary must consult the entity.

6     **30DE Duration of system information periodic reporting notice or**  
7     **system information event-based reporting notice**

8             (1) A system information periodic reporting notice or a system  
9             information event-based reporting notice:

10                 (a) comes into force:

11                     (i) when it is given; or

12                     (ii) if a later time is specified in the notice—at that later  
13                     time; and

14                 (b) remains in force for the period specified in the notice.

15             (2) The period specified in the notice must not be longer than 12  
16             months.

17             (3) If a system information periodic reporting notice (the *original*  
18             *notice*) is in force, this Act does not prevent the Secretary from  
19             giving a fresh system information periodic reporting notice that:

20                 (a) is in the same, or substantially the same, terms as the original  
21                 notice; and

22                 (b) comes into force immediately after the expiry of the original  
23                 notice.

24             (4) If a system information event-based reporting notice (the *original*  
25             *notice*) is in force, this Act does not prevent the Secretary from  
26             giving a fresh system information event-based reporting notice  
27             that:

28                 (a) is in the same, or substantially the same, terms as the original  
29                 notice; and

30                 (b) comes into force immediately after the expiry of the original  
31                 notice.

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1     **30DF Compliance with system information periodic reporting notice**  
2             **or system information event-based reporting notice**

3             An entity must comply with:

- 4                 (a) a system information periodic reporting notice; or  
5                 (b) a system information event-based reporting notice;  
6             to the extent that the entity is capable of doing so.

7             Civil penalty:             200 penalty units.

8     **30DG Self-incrimination etc.**

- 9             (1) An entity is not excused from giving a report under section 30DB  
10             or 30DC on the ground that the report might tend to incriminate the  
11             entity.
- 12             (2) If, at general law, an individual would otherwise be able to claim  
13             the privilege against self-exposure to a penalty (other than a  
14             penalty for an offence) in relation to giving a report under  
15             section 30DB or 30DC, the individual is not excused from giving a  
16             report under that section on that ground.

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

19     **30DH Admissibility of report etc.**

20             If a report is given under section 30DB or 30DC:

- 21                 (a) the report; or  
22                 (b) giving the report;  
23             is not admissible in evidence against an entity:
- 24                 (c) in criminal proceedings other than proceedings for an offence  
25                 against section 137.2 of the *Criminal Code* that relates to this  
26                 Act; or  
27                 (d) in civil proceedings other than proceedings for recovery of a  
28                 penalty in relation to a contravention of section 30DF.

# EXPOSURE DRAFT

Schedule 1 Security of critical infrastructure

Part 1 General amendments

---

1 **Subdivision B—System information software**

2 **30DJ Secretary may require installation of system information**  
3 **software**

4 *Scope*

- 5 (1) This section applies if:
- 6 (a) a computer:
- 7 (i) is needed to operate a system of national significance;
- 8 or
- 9 (ii) is a system of national significance; and
- 10 (b) the Secretary believes on reasonable grounds that the
- 11 responsible entity for the system of national significance
- 12 would not be technically capable of preparing reports under
- 13 section 30DB or 30DC consisting of information that:
- 14 (i) relates to the operation of the computer; and
- 15 (ii) may assist with determining whether a power under this
- 16 Act should be exercised in relation to the system of
- 17 national significance; and
- 18 (iii) is not personal information (within the meaning of the
- 19 *Privacy Act 1988*).

20 *Requirement*

- 21 (2) The Secretary may, by written notice given to the entity, require
- 22 the entity to:
- 23 (a) both:
- 24 (i) install a specified computer program on the computer;
- 25 and
- 26 (ii) do so within the period specified in the notice; and
- 27 (b) maintain the computer program installed in accordance with
- 28 paragraph (a); and
- 29 (c) take all reasonable steps to ensure that the computer is
- 30 continuously supplied with an internet carriage service that
- 31 enables the computer program to function.
- 32 (3) A notice under subsection (2) is to be known as a ***system***
- 33 ***information software notice***.
-



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (4) In deciding whether to give a system information software notice  
2 to the entity, the Secretary must have regard to:  
3 (a) the costs that are likely to be incurred by the entity in  
4 complying with the notice; and  
5 (b) such other matters (if any) as the Secretary considers  
6 relevant.
- 7 (5) A computer program may only be specified in a system  
8 information software notice if the purpose of the computer  
9 program is to:  
10 (a) collect and record information that:  
11 (i) relates to the operation of the computer; and  
12 (ii) may assist with determining whether a power under this  
13 Act should be exercised in relation to the system of  
14 national significance; and  
15 (iii) is not personal information (within the meaning of the  
16 *Privacy Act 1988*); and  
17 (b) cause the information to be transmitted electronically to  
18 ASD.

19 *Matters to be set out in notice*

- 20 (6) A system information software notice must set out the effect of  
21 section 30DM.

22 *Other powers not limited*

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

## 25 **30DK Consultation**

26 Before giving a system information software notice to an entity,  
27 the Secretary must consult the entity.

## 28 **30DL Duration of system information software notice**

- 29 (1) A system information software notice:  
30 (a) comes into force:  
31 (i) when it is given; or

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (ii) if a later time is specified in the notice—at that later  
2 time; and  
3 (b) remains in force for the period specified in the notice.
- 4 (2) The period specified in the notice must not be longer than 12  
5 months.
- 6 (3) If a system information software notice (the *original notice*) is in  
7 force, this Act does not prevent the Secretary from giving a fresh  
8 system information software notice that:  
9 (a) is in the same, or substantially the same, terms as the original  
10 notice; and  
11 (b) comes into force immediately after the expiry of the original  
12 notice.

### 13 **30DM Compliance with system information software notice**

14 An entity must comply with a system information software notice  
15 to the extent that the entity is capable of doing so.

16 Civil penalty: 200 penalty units.

### 17 **30DN Self-incrimination etc.**

- 18 (1) An entity is not excused from complying with a system  
19 information software notice on the ground that complying with the  
20 notice might tend to incriminate the entity.
- 21 (2) If, at general law, an individual would otherwise be able to claim  
22 the privilege against self-exposure to a penalty (other than a  
23 penalty for an offence) in relation to complying with a system  
24 information software notice, the individual is not excused from  
25 complying with the notice on that ground.

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

### 28 **30DP Admissibility of information etc.**

29 If:

- 30 (a) a computer program is installed in compliance with a system  
31 information software notice; and
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (b) information is transmitted to the Secretary as a result of the  
2 operation of the computer program;  
3 the information is not admissible in evidence against an entity in  
4 civil proceedings other than proceedings for recovery of a penalty  
5 in relation to a contravention of section 30DM.

## 6 **Division 6—Designated officers**

### 7 **30DQ Designated officer**

- 8 (1) A *designated officer* is an individual appointed by the Secretary, in  
9 writing, to be a designated officer for the purposes of this Act.
- 10 (2) The Secretary must not appoint an individual under subsection (1)  
11 unless:
- 12 (a) the individual is an APS employee in the Department; or  
13 (b) the individual is a staff member of ASD (within the meaning  
14 of the *Intelligence Services Act 2001*).

### 15 **40 Paragraph 32(4)(c)**

16 Omit “industry for the critical infrastructure asset”, substitute “critical  
17 infrastructure sector”.

### 18 **41 At the end of section 32**

19 Add:

20 *Other powers not limited*

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

### 23 **42 Subparagraph 33(1)(a)(i)**

24 Before “located”, insert “wholly or partly”.

### 25 **43 Subparagraph 33(1)(a)(ii)**

26 Omit “industry for the critical infrastructure asset”, substitute “critical  
27 infrastructure sector”.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 **44 At the end of Part 3**

2 Add:

3 **35AAA Directions prevail over inconsistent critical infrastructure**  
4 **risk management programs**

5 If a critical infrastructure risk management program is applicable  
6 to a critical infrastructure asset, the program has no effect to the  
7 extent to which it is inconsistent with a direction under  
8 subsection 32(2).

9 **35AAB Liability**

- 10 (1) An entity is not liable to an action or other proceeding for damages  
11 for or in relation to an act done or omitted in good faith in  
12 compliance with a direction under subsection 32(2).
- 13 (2) An officer, employee or agent of an entity is not liable to an action  
14 or other proceeding for damages for or in relation to an act done or  
15 omitted in good faith in connection with an act done or omitted by  
16 the entity as mentioned in subsection (1) of this section.

17 **45 After Part 3**

18 Insert:

19 **Part 3A—Responding to serious cyber security**  
20 **incidents**

21 **Division 1—Simplified outline of this Part**

22 **35AA Simplified outline of this Part**

- 23
- 24
- 25
- 26
- 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

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (ii) the defence of Australia; or  
2 (iii) national security; and  
3 (d) no existing regulatory system of the Commonwealth, a State  
4 or a Territory could be used to provide a practical and  
5 effective response to the incident.

#### 6 *Authorisation*

- 7 (2) The Minister may, on application by the Secretary, do any or all of  
8 the following things:  
9 (a) authorise the Secretary to give directions to a specified entity  
10 under section 35AK that relate to the incident and the  
11 primary asset;  
12 (b) authorise the Secretary to give directions to a specified entity  
13 under section 35AK that relate to the incident and a specified  
14 critical infrastructure sector asset;  
15 (c) authorise the Secretary to give to a specified entity a  
16 specified direction under section 35AQ that relates to the  
17 incident and the primary asset;  
18 (d) authorise the Secretary to give to a specified entity a  
19 specified direction under section 35AQ that relates to the  
20 incident and a specified critical infrastructure sector asset;  
21 (e) authorise the Secretary to give a specified request under  
22 section 35AX that relates to the incident and the primary  
23 asset;  
24 (f) authorise the Secretary to give a specified request under  
25 section 35AX that relates to the incident and a specified  
26 critical infrastructure sector asset.

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

28 Note 2: Section 35AQ deals with action directions.

29 Note 3: Section 35AX deals with intervention requests.

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

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

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

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1

## *Information gathering directions*

2

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

3

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

4

5

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

6

(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.

7

8

9

10

11

## *Action directions*

12

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

13

14

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

15

16

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

17

18

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

19

20

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

21

22

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

23

24

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

25

26

(a) the impact of the specified direction on:

27

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

28

(ii) the functioning of the asset concerned; and

29

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

30

31

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

32

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

33

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (a) requires the specified entity to permit the authorised agency  
2 to do an act or thing that could be the subject of a request  
3 under section 35AX; or  
4 (b) requires the specified entity to take offensive cyber action  
5 against a person who is directly or indirectly responsible for  
6 the incident.

7 *Intervention requests*

- 8 (10) The Minister must not give a Ministerial authorisation under  
9 paragraph (2)(e) or (f) unless the Minister is satisfied that:  
10 (a) giving a Ministerial authorisation under paragraph (2)(c) or  
11 (d) would not amount to a practical and effective response to  
12 the incident; and  
13 (b) if there is only one relevant entity for the asset concerned—  
14 the relevant entity is unwilling or unable take all reasonable  
15 steps to resolve the incident; and  
16 (c) if there are 2 or more relevant entities for the asset  
17 concerned—those entities, when considered together, are  
18 unwilling or unable take all reasonable steps to resolve the  
19 incident; and  
20 (d) the specified request is reasonably necessary for the purposes  
21 of responding to the incident; and  
22 (e) the specified request is a proportionate response to the  
23 incident; and  
24 (f) compliance with the specified request is technically feasible;  
25 and  
26 (g) each of the acts or things specified in the specified request is  
27 an act or thing of a kind covered by section 35AC.

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

- 30 (11) In determining whether the specified request is a proportionate  
31 response to the incident, the Minister must have regard to:  
32 (a) the impact of compliance with the specified request on the  
33 functioning of the asset concerned; and  
34 (b) the consequences of acts or things that would be done in  
35 compliance with the specified request; and  
36 (c) such other matters (if any) as the Minister considers relevant.



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (12) The Minister must not give a Ministerial authorisation under  
2 paragraph (2)(e) or (f) if compliance with the specified request  
3 would involve the authorised agency taking offensive cyber action  
4 against a person who is directly or indirectly responsible for the  
5 incident.
- 6 (13) The Minister must not give a Ministerial authorisation under  
7 paragraph (2)(e) or (f) unless the Minister has obtained the  
8 agreement of:  
9 (a) the Prime Minister; and  
10 (b) the Defence Minister.
- 11 (14) An agreement under subsection (13) may be given:  
12 (a) orally; or  
13 (b) in writing.
- 14 (15) If an agreement under subsection (13) is given orally, the Prime  
15 Minister or the Defence Minister, as the case requires, must:  
16 (a) do both of the following:  
17 (i) make a written record of the agreement;  
18 (ii) give a copy of the written record of the agreement to the  
19 Minister; and  
20 (b) do so within 48 hours after the agreement is given.
- 21 *Ministerial authorisation is not a legislative instrument*
- 22 (16) A Ministerial authorisation is not a legislative instrument.
- 23 *Other powers not limited*
- 24 (17) This section does not, by implication, limit a power conferred by  
25 another provision of this Act.

## 26 **35AC Kinds of acts or things that may be specified in an** 27 **intervention request**

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (i) a computer that is, or is part of, the asset to which the  
2 Ministerial authorisation relates; or
- 3 (ii) a computer device that is, or is part of, the asset to  
4 which the Ministerial authorisation relates;
- 5 (b) undertake an analysis of:
- 6 (i) a computer that is, or is part of, the asset to which the  
7 Ministerial authorisation relates; or
- 8 (ii) a computer program that is, or is part of, the asset to  
9 which the Ministerial authorisation relates; or
- 10 (iii) computer data that is, or is part of, the asset to which the  
11 Ministerial authorisation relates; or
- 12 (iv) a computer device that is, or is part of, the asset to  
13 which the Ministerial authorisation relates;
- 14 (c) if it is necessary to achieve the purpose mentioned in  
15 paragraph (b)—install a computer program on a computer  
16 that is, or is part of, the asset to which the Ministerial  
17 authorisation relates;
- 18 (d) access, add, restore, copy, alter or delete data held in:
- 19 (i) a computer that is, or is part of, the asset to which the  
20 Ministerial authorisation relates; or
- 21 (ii) a computer device that is, or is part of, the asset to  
22 which the Ministerial authorisation relates;
- 23 (e) access, restore, copy, alter or delete a computer program that  
24 is, or is part of, the asset to which the Ministerial  
25 authorisation relates;
- 26 (f) access, copy, alter or delete a computer program that is  
27 installed on a computer that is, or is part of, the asset to  
28 which the Ministerial authorisation relates;
- 29 (g) alter the functioning of:
- 30 (i) a computer that is, or is part of, the asset to which the  
31 Ministerial authorisation relates; or
- 32 (ii) a computer device that is, or is part of, the asset to  
33 which the Ministerial authorisation relates;
- 34 (h) remove or disconnect:
- 35 (i) a computer; or
- 36 (ii) a computer device;
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 from a computer network that is, or is part of, the asset to  
2 which the Ministerial authorisation relates;
- 3 (i) connect or add:
- 4 (i) a computer; or  
5 (ii) a computer device;
- 6 to a computer network that is, or is part of, the asset to which  
7 the Ministerial authorisation relates;
- 8 (j) remove:
- 9 (i) a computer that is, or is part of, the asset to which the  
10 Ministerial authorisation relates; or  
11 (ii) a computer device that is, or is part of, the asset to  
12 which the Ministerial authorisation relates;
- 13 from premises.

## 14 **35AD Consultation**

- 15 (1) Before giving a Ministerial authorisation under  
16 paragraph 35AB(2)(c) or (d), the Minister must consult the  
17 specified entity unless the delay that would occur if the specified  
18 entity were consulted would frustrate the effectiveness of the  
19 Ministerial authorisation.
- 20 (2) Before giving a Ministerial authorisation under  
21 paragraph 35AB(2)(e) or (f) in relation to an asset, the Minister  
22 must:
- 23 (a) if the asset is a critical infrastructure asset—consult the  
24 responsible entity for the asset; or  
25 (b) if the asset is a critical infrastructure sector asset (other than a  
26 critical infrastructure asset)—consult whichever of the  
27 following entities the Minister considers to be most relevant  
28 in relation to the proposed authorisation:
- 29 (i) the owner, or each of the owners, of the asset;  
30 (ii) the operator, or each of the operators, of the asset;
- 31 unless the delay that would occur if the entity or entities were  
32 consulted would frustrate the effectiveness of the Ministerial  
33 authorisation.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

#### 1 **35AE Form and notification of Ministerial authorisation**

2 (1) A Ministerial authorisation may be given:

3 (a) orally; or

4 (b) in writing.

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

7 (a) a cyber security incident; and

8 (b) an asset;

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

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

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

#### 15 *Notification of Ministerial authorisations given orally*

16 (3) If a Ministerial authorisation is given orally in relation to:

17 (a) a cyber security incident; and

18 (b) an asset;

19 the Minister must:

20 (c) do both of the following:

21 (i) make a written record of the Ministerial authorisation;

22 (ii) give a copy of the written record of the Ministerial  
23 authorisation to the Secretary and the Inspector-General  
24 of Intelligence and Security; and

25 (d) do so within 48 hours after the Ministerial authorisation is  
26 given.

27 (4) If a Ministerial authorisation is given orally in relation to:

28 (a) a cyber security incident; and

29 (b) a critical infrastructure asset;

30 the Minister must:

31 (c) do both of the following:

32 (i) make a written record of the Ministerial authorisation;

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (ii) give a copy of the written record of the Ministerial  
2 authorisation to the responsible entity for the asset; and  
3 (d) do so within 48 hours after the Ministerial authorisation is  
4 given.
- 5 (5) If a Ministerial authorisation is given orally in relation to:  
6 (a) a cyber security incident; and  
7 (b) a critical infrastructure sector asset (other than a critical  
8 infrastructure asset);  
9 the Minister must:  
10 (c) make a written record of the Ministerial authorisation; and  
11 (d) give a copy of the written record of the Ministerial  
12 authorisation to whichever of the following entities the  
13 Minister considers to be most relevant in relation to the  
14 Ministerial authorisation:  
15 (i) the owner, or each of the owners, of the asset;  
16 (ii) the operator, or each of the operators, of the asset; and  
17 (e) do so within 48 hours after the Ministerial authorisation is  
18 given.

19 *Notification of Ministerial authorisations given in writing*

- 20 (6) If a Ministerial authorisation is given in writing in relation to:  
21 (a) a cyber security incident; and  
22 (b) an asset;  
23 the Minister must:  
24 (c) give a copy of the Ministerial authorisation to the Secretary  
25 and the Inspector-General of Intelligence and Security; and  
26 (d) do so within 48 hours after the Ministerial authorisation is  
27 given.
- 28 (7) If a Ministerial authorisation is given in writing in relation to:  
29 (a) a cyber security incident; and  
30 (b) a critical infrastructure asset;  
31 the Minister must:  
32 (c) give a copy of the Ministerial authorisation to the responsible  
33 entity for the asset; and

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

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

#### 15 **35AF Form of application for Ministerial authorisation**

- 16 (1) The Secretary may apply for a Ministerial authorisation either:  
17 (a) orally; or  
18 (b) in writing.
- 19 (2) The Secretary must not apply orally for a Ministerial authorisation  
20 that relates to:  
21 (a) a cyber security incident; and  
22 (b) an asset;  
23 unless the delay that would occur if the application were to be  
24 made in writing would frustrate the effectiveness of:  
25 (c) any directions that may be given under section 35AK  
26 or 35AQ in relation to the incident and the asset; or  
27 (d) any requests that may be given under section 35AX in  
28 relation to the incident and the asset.
- 29 (3) If an application for a Ministerial authorisation is made orally, the  
30 Secretary must:  
31 (a) do both of the following:  
32 (i) make a written record of the application;  
33 (ii) give a copy of the written record of the application to  
34 the Minister; and

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 (b) do so within 48 hours after the application is made.

## 2 **35AG Duration of Ministerial authorisation**

### 3 *Scope*

4 (1) This section applies if a Ministerial authorisation is given in  
5 relation to:

- 6 (a) a cyber security incident; and  
7 (b) an asset.

### 8 *Duration of Ministerial authorisation*

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

### 12 *Fresh Ministerial authorisation*

13 (3) If a Ministerial authorisation (the ***original Ministerial***  
14 ***authorisation***) is in force, this Act does not prevent the Minister  
15 from giving a fresh Ministerial authorisation that:

- 16 (a) is in the same, or substantially the same, terms as the original  
17 Ministerial authorisation; and  
18 (b) comes into force immediately after the expiry of the original  
19 Ministerial authorisation.

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

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

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 **35AH Revocation of Ministerial authorisation**

2 *Scope*

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

7 *Power to revoke Ministerial authorisation*

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

9 *Duty to revoke Ministerial authorisation*

- 10 (3) If the Minister is satisfied that the Ministerial authorisation is no  
11 longer required to respond to the incident, the Minister must, in  
12 writing, revoke the Ministerial authorisation.
- 13 (4) If the Secretary is satisfied that the Ministerial authorisation is no  
14 longer required to respond to the incident, the Secretary must:  
15 (a) notify the Minister that the Secretary is so satisfied; and  
16 (b) do so soon as practicable after the Secretary becomes so  
17 satisfied.

18 *Notification of revocation*

- 19 (5) If the Ministerial authorisation is revoked, the Minister must:  
20 (a) give a copy of the revocation to:  
21 (i) the Secretary; and  
22 (ii) the Inspector-General of Intelligence and Security; and  
23 (iii) each relevant entity for the asset; and  
24 (b) do so within 48 hours after the Ministerial authorisation is  
25 revoked.
- 26 (6) If a Ministerial authorisation is revoked in relation to:  
27 (a) a cyber security incident; and  
28 (b) a critical infrastructure asset;  
29 the Minister must:
-



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (c) give a copy of the revocation to the responsible entity for the  
2 asset; and  
3 (d) do so within 48 hours after the Ministerial authorisation is  
4 revoked.

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

17 *Revocation is not a legislative instrument*

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

20 *Application of Acts Interpretation Act 1901*

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

## 25 **35AJ Minister to exercise powers personally**

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

# EXPOSURE DRAFT

Schedule 1 Security of critical infrastructure

Part 1 General amendments

---

1 **Division 3—Information gathering directions**

2 **35AK Information gathering direction**

3 *Scope*

4 (1) This section applies if a Ministerial authorisation given under  
5 paragraph 35AB(2)(a) or (b) is in force in relation to:

- 6 (a) a cyber security incident; and  
7 (b) an asset.

8 *Direction*

9 (2) If:

- 10 (a) an entity is a relevant entity for the asset; and  
11 (b) the Secretary has reason to believe that the entity has  
12 information that may assist with determining whether a  
13 power under this Act should be exercised in relation to the  
14 incident and the asset;

15 the Secretary may direct the entity to:

- 16 (c) give any such information to the Secretary; and  
17 (d) do so within the period, and in the manner, specified in the  
18 direction.

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

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

- 23 (a) the direction is a proportionate means of obtaining the  
24 information; and  
25 (b) compliance with the direction is technically feasible.

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

- 28 (a) do an act or thing that would be prohibited by section 7 of the  
29 *Telecommunications (Interception and Access) Act 1979*; or  
30 (b) do an act or thing that would be prohibited by section 108 of  
31 the *Telecommunications (Interception and Access) Act 1979*;  
32 or
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

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

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

8 *Other powers not limited*

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

## 11 **35AL Form of direction**

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

- 13 (a) orally; or  
14 (b) in writing.

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

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

- 20 (a) do both of the following:  
21 (i) make a written record of the direction;  
22 (ii) give a copy of the written record of the direction to the  
23 entity; and  
24 (b) do so within 48 hours after the direction is given.

## 25 **35AM Compliance with an information gathering direction**

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

28 Civil penalty: 150 penalty units.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 **35AN Self-incrimination etc.**

- 2 (1) An entity is not excused from giving information under  
3 section 35AK on the ground that the information might tend to  
4 incriminate the entity.
- 5 (2) If, at general law, an individual would otherwise be able to claim  
6 the privilege against self-exposure to a penalty (other than a  
7 penalty for an offence) in relation to giving information under  
8 section 35AK, the individual is not excused from giving  
9 information under that section on that ground.

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

12 **35AP Admissibility of information etc.**

- 13 If information is given under section 35AK:
- 14 (a) the information; or  
15 (b) giving the information;
- 16 is not admissible in evidence against an entity:
- 17 (c) in criminal proceedings other than proceedings for an offence  
18 against section 137.1 or 137.2 of the *Criminal Code* that  
19 relates to this Act; or  
20 (d) in civil proceedings other than proceedings for recovery of a  
21 penalty in relation to a contravention of section 35AM.

22 **Division 4—Action directions**

23 **35AQ Action direction**

- 24 (1) If an entity is a relevant entity for:  
25 (a) a critical infrastructure asset; or  
26 (b) a critical infrastructure sector asset;  
27 the Secretary may give the entity a direction that directs the entity  
28 to do, or refrain from doing, a specified act or thing within the  
29 period specified in the direction.
- 30 (2) The Secretary must not give a direction under this section unless  
31 the direction:  
32 (a) is authorised by a Ministerial authorisation; and
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (b) includes a statement to the effect that the direction is  
2 authorised by the Ministerial authorisation; and  
3 (c) specifies the date on which the Ministerial authorisation was  
4 given.

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

- 8 (3) The period specified in the direction must end at or before the end  
9 of the period for which the Ministerial authorisation is in force.  
10 (4) A direction under this section is subject to such conditions (if any)  
11 as are specified in the direction.  
12 (5) The Secretary must not give a direction under this section that  
13 would require an entity to give information to the Secretary.

14 *Other powers not limited*

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

## 17 **35AR Form of direction**

- 18 (1) A direction under section 35AQ may be given:  
19 (a) orally; or  
20 (b) in writing.  
21 (2) The Secretary must not give a direction under section 35AQ orally  
22 unless the delay that would occur if the direction were to be given  
23 in writing would frustrate the effectiveness of the direction.  
24 (3) If a direction under section 35AQ is given orally to an entity, the  
25 Secretary must:  
26 (a) do both of the following:  
27 (i) make a written record of the direction;  
28 (ii) give a copy of the written record of the direction to the  
29 entity; and  
30 (b) do so within 48 hours after the direction is given.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 **35AS Revocation of direction**

2 *Scope*

- 3 (1) This section applies if:  
4 (a) a direction is in force under section 35AQ in relation to a  
5 Ministerial authorisation; and  
6 (b) the direction was given to a particular entity.

7 *Power to revoke direction*

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

10 *Duty to revoke direction*

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

15 *Automatic revocation of direction*

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

18 *Application of Acts Interpretation Act 1901*

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

23 **35AT Compliance with direction**

24 An entity commits an offence if:

- 25 (a) the entity is given a direction under section 35AQ; and  
26 (b) the entity engages in conduct; and  
27 (c) the entity's conduct breaches the direction.

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

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1     **35AU Directions prevail over inconsistent critical infrastructure risk**  
2             **management programs**

3             If a critical infrastructure risk management program is applicable  
4             to an entity, the program has no effect to the extent to which it is  
5             inconsistent with a direction given to the entity under  
6             section 35AQ.

7     **35AV Directions prevail over inconsistent obligations**

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

11    **35AW Liability**

- 12            (1) An entity is not liable to an action or other proceeding for damages  
13            for or in relation to an act done or omitted in good faith in  
14            compliance with a direction given under section 35AQ.
- 15            (2) An officer, employee or agent of an entity is not liable to an action  
16            or other proceeding for damages for or in relation to an act done or  
17            omitted in good faith in connection with an act done or omitted by  
18            the entity as mentioned in subsection (1).

19    **Division 5—Intervention requests**

20    **35AX Intervention request**

- 21            (1) The Secretary may give the chief executive of the authorised  
22            agency a request that the authorised agency do one or more  
23            specified acts or things within the period specified in the request.
- 24            (2) The Secretary must not give a request under this section unless the  
25            request:  
26            (a) is authorised by a Ministerial authorisation; and  
27            (b) includes a statement to the effect that the request is  
28            authorised by the Ministerial authorisation; and  
29            (c) specifies the date on which the Ministerial authorisation was  
30            given.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 Note: A Ministerial authorisation must not be given unless the Minister is  
2 satisfied that the request is reasonably necessary for the purposes of  
3 responding to a cyber security incident—see section 35AB.
- 4 (3) The period specified in the request must end at or before the end of  
5 the period for which the Ministerial authorisation is in force.
- 6 (4) A request under this section is subject to such conditions (if any) as  
7 are specified in the request.
- 8 (5) A request under this section does not extend to:  
9 (a) doing an act or thing that would be prohibited by section 7 of  
10 the *Telecommunications (Interception and Access) Act 1979*;  
11 or  
12 (b) doing an act or thing that would be prohibited by section 108  
13 of the *Telecommunications (Interception and Access) Act*  
14 *1979*; or  
15 (c) doing an act or thing that would (disregarding this Act) be  
16 prohibited by section 276, 277 or 278 of the  
17 *Telecommunications Act 1997*.
- 18 *Other powers not limited*
- 19 (6) This section does not, by implication, limit a power conferred by  
20 another provision of this Act.

#### 21 **35AY Form and notification of request**

- 22 (1) A request under section 35AX may be given:  
23 (a) orally; or  
24 (b) in writing.
- 25 (2) The Secretary must not give a request under section 35AX orally  
26 unless the delay that would occur if the request were to be given in  
27 writing would frustrate the effectiveness of the request.
- 28 *Notification of requests given orally*
- 29 (3) If a request under section 35AX is given orally, the Secretary must:  
30 (a) do both of the following:  
31 (i) make a written record of the request;



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (ii) give a copy of the written record of the request to the  
2 chief executive of the authorised agency; and  
3 (b) do so within 48 hours after the request is given.
- 4 (4) If a request under section 35AX is given orally in relation to a  
5 critical infrastructure asset, the Secretary must:  
6 (a) do both of the following:  
7 (i) make a written record of the request;  
8 (ii) give a copy of the written record of the request to the  
9 responsible entity for the asset; and  
10 (b) do so within 48 hours after the request is given.
- 11 (5) If a request under section 35AX is given orally in relation to a  
12 critical infrastructure sector asset (other than a critical  
13 infrastructure asset), the Secretary must:  
14 (a) make a written record of the request; and  
15 (b) give a copy of the written record of the request to whichever  
16 of the following entities the Secretary considers to be most  
17 relevant in relation to the request:  
18 (i) the owner, or each of the owners, of the asset;  
19 (ii) the operator, or each of the operators, of the asset; and  
20 (c) do so within 48 hours after the request is given.
- 21 *Notification of requests given in writing*
- 22 (6) If a request under section 35AX is given in writing, the Secretary  
23 must:  
24 (a) give a copy of the request to the chief executive of the  
25 authorised agency; and  
26 (b) do so within 48 hours after the request is made.
- 27 (7) If a request under section 35AX is given in writing in relation to a  
28 critical infrastructure asset, the Secretary must:  
29 (a) give a copy of the request to the responsible entity for the  
30 asset; and  
31 (b) do so within 48 hours after the request is given.
- 32 (8) If a request under section 35AX is given in writing in relation to a  
33 critical infrastructure sector asset (other than a critical  
34 infrastructure asset), the Secretary must:
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (a) give a copy of the request to whichever of the following  
2 entities the Secretary considers to be most relevant in relation  
3 to the request:  
4 (i) the owner, or each of the owners, of the asset;  
5 (ii) the operator, or each of the operators, of the asset; and  
6 (b) do so within 48 hours after the request is given.

#### 7 **35AZ Compliance with request**

- 8 (1) The authorised agency is authorised to do an act or thing in  
9 compliance with a request under section 35AX.  
10 (2) An act or thing done by the authorised agency in compliance with a  
11 request under section 35AX is taken to be done in the performance  
12 of the function conferred on the authorised agency by  
13 paragraph 7(1)(f) of the *Intelligence Services Act 2001*.

#### 14 **35BA Revocation of request**

##### 15 *Scope*

- 16 (1) This section applies if a request is in force under section 35AX in  
17 relation to a Ministerial authorisation.

##### 18 *Power to revoke request*

- 19 (2) The Secretary may, by written notice given to the chief executive  
20 of the authorised agency, revoke the request.

##### 21 *Duty to revoke request*

- 22 (3) If the Secretary is satisfied that the request is no longer required to  
23 respond to the cyber security incident to which the Ministerial  
24 authorisation relates, the Secretary must, by written notice given to  
25 the chief executive of the authorised agency, revoke the request.

##### 26 *Automatic revocation of request*

- 27 (4) If the Ministerial authorisation ceases to be in force, the request is  
28 revoked.



# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

#### 1 **35BC Constable may assist the authorised agency**

- 2 (1) If an entity refuses or fails to provide a staff member of the  
3 authorised agency with access to premises when required to do so  
4 under subsection 35BB(1):
- 5 (a) the staff member may enter the premises for the purposes of  
6 the authorised agency complying with the request mentioned  
7 in that subsection; and
- 8 (b) a constable may:
- 9 (i) assist the staff member in gaining access to the premises  
10 by using reasonable force against property; and
- 11 (ii) if necessary for the purposes of so assisting the staff  
12 member—enter the premises.
- 13 (2) If a staff member of the authorised agency has entered premises for  
14 the purposes of the authorised agency complying with a request  
15 under section 35AX, a constable may:
- 16 (a) assist the authorised agency in complying with the request by  
17 using reasonable force against property located on the  
18 premises; and
- 19 (b) for the purposes of so assisting the authorised agency—enter  
20 the premises.

#### 21 **35BD Removal and return of computers etc.**

##### 22 *Removal of computers etc.*

- 23 (1) If:
- 24 (a) in compliance with a request under section 35AX, the  
25 authorised agency adds or connects a computer or device to a  
26 computer network; and
- 27 (b) at a time when the request is in force, a staff member of the  
28 authorised agency forms a reasonable belief that the addition  
29 or connection of the computer or device is no longer required  
30 for the purposes of responding to the cyber security incident  
31 to which the relevant Ministerial authorisation relates;
- 32 the authorised agency must remove or disconnect the computer or  
33 device as soon as practicable after the staff member forms that  
34 belief.

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (2) If:  
2 (a) in compliance with a request under section 35AX, the  
3 authorised agency adds or connects a computer or device to a  
4 computer network; and  
5 (b) the request ceases to be in force;  
6 the authorised agency must remove or disconnect the computer or  
7 device as soon as practicable after the request ceases to be in force.

8 *Return of computers etc.*

- 9 (3) If:  
10 (a) in compliance with a request under section 35AX, the  
11 authorised agency removes a computer or device; and  
12 (b) at a time when the request is in force, a staff member of the  
13 authorised agency forms a reasonable belief that the removal  
14 of the computer or device is no longer required for the  
15 purposes of responding to the cyber security incident to  
16 which the relevant Ministerial authorisation relates;  
17 the authorised agency must return the computer or device as soon  
18 as practicable after the staff member forms that belief.

- 19 (4) If:  
20 (a) in compliance with a request under section 35AX, the  
21 authorised agency removes a computer or device; and  
22 (b) the request ceases to be in force;  
23 the authorised agency must return the computer or device as soon  
24 as practicable after the request ceases to be in force.

## 25 **35BE Use of force against an individual not authorised**

26 This Division does not authorise the use of force against an  
27 individual.

## 28 **35BF Liability**

- 29 Each of the following:  
30 (a) the chief executive of the authorised agency;  
31 (b) a staff member of the authorised agency;  
32 (c) a constable;
-

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 is not liable to an action or other proceeding (whether civil or  
2 criminal) for, or in relation to, an act or matter in good faith done  
3 or omitted to be done in the exercise, or purported exercise, of any  
4 power or authority conferred by this Division.

#### 5 **35BG Evidentiary certificates**

6 (1) The Inspector-General of Intelligence and Security may issue a  
7 written certificate setting out any facts the Inspector-General of  
8 Intelligence and Security considers relevant with respect to  
9 anything done, or omitted to be done, by the authorised agency, or  
10 a staff member of the authorised agency, in the exercise of any  
11 power or authority conferred by this Division.

12 (2) A certificate issued under subsection (1) is admissible in evidence  
13 in any proceedings as prima facie evidence of the matters stated in  
14 the certificate.

#### 15 **35BH Chief executive of the authorised agency to report to the** 16 **Minister and the Defence Minister**

17 (1) If:  
18 (a) the Secretary gives a request under section 35AX that was  
19 authorised by a Ministerial authorisation; and  
20 (b) the authorised agency does one or more acts or things in  
21 compliance with the request;  
22 the chief executive of the authorised agency must:  
23 (c) prepare a written report that:  
24 (i) sets out details of those acts or things; and  
25 (ii) explains the extent to which doing those acts or things  
26 has amounted to an effective response to the cyber  
27 security incident to which the Ministerial authorisation  
28 relates; and  
29 (d) give a copy of the report to the Minister; and  
30 (e) give a copy of the report to the Defence Minister.

31 (2) The chief executive of the authorised agency must comply with  
32 subsection (1) as soon as practicable after the end of the period  
33 specified in the request and, in any event, within 3 months after the  
34 end of the period specified in the request.

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 **46 Section 36 (paragraph beginning “Information”)**

2 Repeal the paragraph.

3 **47 At the end of section 36**

4 Add:

5 Note: Protected information is defined in section 5.

6 **48 Subparagraph 42(2)(a)(viii)**

7 Omit “industry for the critical infrastructure asset”, substitute “critical  
8 infrastructure sector”.

9 **49 Paragraph 42(2)(b)**

10 Omit “industry for the critical infrastructure asset”, substitute “critical  
11 infrastructure sector”.

12 **50 After section 43**

13 Insert:

14 **43A Authorised use and disclosure—Ombudsman official**

15 Protected information may be disclosed by an Ombudsman official  
16 to an IGIS official for the purposes of the IGIS official exercising  
17 powers, or performing functions or duties, as an IGIS official.

18 **43B Authorised use and disclosure—IGIS official**

19 Protected information may be disclosed by an IGIS official to an  
20 Ombudsman official for the purposes of the Ombudsman official  
21 exercising powers, or performing functions or duties, as an  
22 Ombudsman official.

23 **43C Authorised use and disclosure—ASD**

24 The Director-General of ASD or a staff member of ASD may make  
25 a record of, use or disclose protected information for the purposes  
26 of the performance of the functions of ASD set out in section 7 of  
27 the *Intelligence Services Act 2001*.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 **51 Paragraph 45(1)(a)**

2 After “obtains”, insert “or generates”.

3 **52 Paragraph 45(1)(d)**

4 Omit “subsection 51(3) or 52(4)”, substitute “a notification provision”.

5 **53 Paragraph 46(1)(a)**

6 Omit “subsection 51(3) or 52(4)”, substitute “a notification provision”.

7 **54 Subsection 46(3)**

8 Omit “subsection 51(3) or 52(4)”, substitute “a notification provision”.

9 **55 At the end of section 48**

10 Add:

11 Infringement notices may be given under Part 5 of the Regulatory  
12 Powers Act for alleged contraventions of certain provisions of this  
13 Act.

14 A provision is subject to monitoring under Part 2 of the Regulatory  
15 Powers Act if it is:

- 16 (a) an offence against section 35AT or 45 of this Act; or  
17 (b) a civil penalty provision of this Act.

18 A provision is subject to investigation under Part 3 of the  
19 Regulatory Powers Act if it is:

- 20 (a) an offence against section 35AT or 45 of this Act; or  
21 (b) a civil penalty provision of this Act.

22 **56 Subsections 49(2) and (3)**

23 Repeal the subsections, substitute:

24 *Authorised applicant*

- 25 (2) For the purposes of Part 4 of the Regulatory Powers Act, as that  
26 Part applies in relation to a civil penalty provision of this Act, each  
27 of the following persons is an authorised applicant:



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (a) the Secretary;  
2 (b) a person who is appointed under subsection (3).
- 3 (3) The Secretary may, by writing, appoint a person who:  
4 (a) is the chief executive officer (however described) of a  
5 relevant Commonwealth regulator; or  
6 (b) is an SES employee, or an acting SES employee, in:  
7 (i) the Department; or  
8 (ii) a relevant Commonwealth regulator; or  
9 (c) holds, or is acting in, a position in a relevant Commonwealth  
10 regulator that is equivalent to, or higher than, a position  
11 occupied by an SES employee;  
12 to be an authorised applicant for the purposes of Part 4 of the  
13 Regulatory Powers Act, as that Part applies in relation to a civil  
14 penalty provision of this Act.

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

## 17 *Authorised person*

- 18 (3A) For the purposes of Parts 6 and 7 of the Regulatory Powers Act, as  
19 those Parts apply in relation to a civil penalty provision of this Act,  
20 each of the following persons is an authorised applicant:  
21 (a) the Secretary;  
22 (b) a person who is appointed under subsection (3B).
- 23 (3B) The Secretary may, by writing, appoint a person who:  
24 (a) is the chief executive officer (however described) of a  
25 relevant Commonwealth regulator; or  
26 (b) is an SES employee, or an acting SES employee, in:  
27 (i) the Department; or  
28 (ii) a relevant Commonwealth regulator; or  
29 (c) holds, or is acting in, a position in a relevant Commonwealth  
30 regulator that is equivalent to, or higher than, a position  
31 occupied by an SES employee;  
32 to be an authorised applicant for the purposes of Parts 6 and 7 of  
33 the Regulatory Powers Act, as those Parts apply in relation to a  
34 civil penalty provision of this Act.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

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

### 3 **57 At the end of Part 5**

4 Add:

## 5 **Division 3—Monitoring and investigation powers**

### 6 **49A Monitoring powers**

#### 7 *Provisions subject to monitoring*

- 8 (1) A provision is subject to monitoring under Part 2 of the Regulatory  
9 Powers Act if it is:  
10 (a) an offence against section 35AT or 45; or  
11 (b) a civil penalty provision of this Act.

12 Note: Part 2 of the Regulatory Powers Act creates a framework for  
13 monitoring whether the provisions have been complied with. It  
14 includes powers of entry and inspection.

#### 15 *Information subject to monitoring*

- 16 (2) Information given in compliance or purported compliance with a  
17 provision of this Act is subject to monitoring under Part 2 of the  
18 Regulatory Powers Act.

19 Note: Part 2 of the Regulatory Powers Act creates a framework for  
20 monitoring whether the information is correct. It includes powers of  
21 entry and inspection.

#### 22 *Authorised applicant*

- 23 (3) For the purposes of Part 2 of the Regulatory Powers Act, a person  
24 who is appointed under subsection (4) is an authorised applicant in  
25 relation to the provisions mentioned in subsection (1) and  
26 information mentioned in subsection (2).
- 27 (4) The Secretary may, by writing, appoint a person who:  
28 (a) is an SES employee, or an acting SES employee, in:  
29 (i) the Department; or  
30 (ii) a relevant Commonwealth regulator; or
-

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 (b) holds, or is acting in, a position in a relevant Commonwealth  
2 regulator that is equivalent to, or higher than, a position  
3 occupied by an SES employee;  
4 to be an authorised applicant in relation to the provisions  
5 mentioned in subsection (1) and information mentioned in  
6 subsection (2).

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

9 *Authorised person*

10 (5) For the purposes of Part 2 of the Regulatory Powers Act, a person  
11 who is appointed under subsection (6) is an authorised person in  
12 relation to the provisions mentioned in subsection (1) and  
13 information mentioned in subsection (2).

14 (6) The Secretary may, by writing, appoint a person who is:

15 (a) an APS employee in:

16 (i) the Department; or

17 (ii) a relevant Commonwealth regulator; or

18 (b) an officer or employee of a relevant Commonwealth  
19 regulator;

20 to be an authorised person in relation to the provisions mentioned  
21 in subsection (1) and information mentioned in subsection (2).

22 *Issuing officer*

23 (7) For the purposes of Part 2 of the Regulatory Powers Act, a  
24 magistrate is an issuing officer in relation to the provisions  
25 mentioned in subsection (1) and information mentioned in  
26 subsection (2).

27 *Relevant chief executive*

28 (8) For the purposes of Part 2 of the Regulatory Powers Act, the  
29 Secretary is the relevant chief executive in relation to the  
30 provisions mentioned in subsection (1) and information mentioned  
31 in subsection (2).

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 (9) The relevant chief executive may, in writing, delegate the powers  
2 and functions mentioned in subsection (10) to a person who is an  
3 SES employee, or an acting SES employee, in the Department.

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

6 (10) The powers and functions that may be delegated are:

7 (a) powers under Part 2 of the Regulatory Powers Act in relation  
8 to the provisions mentioned in subsection (1) and information  
9 mentioned in subsection (2); and

10 (b) powers and functions under the Regulatory Powers Act that  
11 are incidental to a power mentioned in paragraph (a).

12 (11) A person exercising powers or performing functions under a  
13 delegation under subsection (9) must comply with any directions of  
14 the relevant chief executive.

#### 15 *Relevant court*

16 (12) For the purposes of Part 2 of the Regulatory Powers Act, each of  
17 the following courts is a relevant court in relation to the provisions  
18 mentioned in subsection (1) and information mentioned in  
19 subsection (2):

20 (a) the Federal Court of Australia;

21 (b) the Federal Circuit Court of Australia; and

22 (c) a court of a State or Territory that has jurisdiction in relation  
23 to matters arising under this Act.

#### 24 *Premises*

25 (13) An authorised person must not enter premises under Part 2 of the  
26 Regulatory Powers Act, as it applies in relation to the provisions  
27 mentioned in subsection (1) and information mentioned in  
28 subsection (2), if the premises are used solely or primarily as a  
29 residence.

#### 30 *Person assisting*

31 (14) An authorised person may be assisted by other persons in  
32 exercising powers, or performing functions or duties, under Part 2  
33 of the Regulatory Powers Act in relation to the provisions

---

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 mentioned in subsection (1) and information mentioned in  
2 subsection (2).

## 3 *External Territories*

4 (15) Part 2 of the Regulatory Powers Act, as it applies in relation to the  
5 provisions mentioned in subsection (1) and information mentioned  
6 in subsection (2), extends to every external Territory.

## 7 **49B Investigation powers**

### 8 *Provisions subject to investigation*

- 9 (1) A provision is subject to investigation under Part 3 of the  
10 Regulatory Powers Act if it is:  
11 (a) an offence against section 35AT or 45; or  
12 (b) a civil penalty provision of this Act.

### 13 *Authorised applicant*

14 (2) For the purposes of Part 3 of the Regulatory Powers Act, a person  
15 who is appointed under subsection (3) is an authorised applicant in  
16 relation to evidential material that relates to a provision mentioned  
17 in subsection (1).

18 (3) The Secretary may, by writing, appoint a person who:  
19 (a) is an SES employee, or an acting SES employee, in:  
20 (i) the Department; or  
21 (ii) a relevant Commonwealth regulator; or  
22 (b) holds, or is acting in, a position in a relevant Commonwealth  
23 regulator that is equivalent to, or higher than, a position  
24 occupied by an SES employee;  
25 to be an authorised applicant in relation to evidential material that  
26 relates to a provision mentioned in subsection (1).

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

### 29 *Authorised person*

30 (4) For the purposes of Part 3 of the Regulatory Powers Act, a person  
31 who is appointed under subsection (5) is an authorised person in

---

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 relation to evidential material that relates to a provision mentioned  
2 in subsection (1).

3 (5) The Secretary may, by writing, appoint a person who is:

4 (a) an APS employee in:

5 (i) the Department; or

6 (ii) a relevant Commonwealth regulator; or

7 (b) an officer or employee of a relevant Commonwealth  
8 regulator;

9 to be an authorised person in relation to evidential material that  
10 relates to a provision mentioned in subsection (1).

11 *Issuing officer*

12 (6) For the purposes of Part 3 of the Regulatory Powers Act, a  
13 magistrate is an issuing officer in relation to evidential material  
14 that relates to a provision mentioned in subsection (1).

15 *Relevant chief executive*

16 (7) For the purposes of Part 3 of the Regulatory Powers Act, the  
17 Secretary is the relevant chief executive in relation to evidential  
18 material that relates to a provision mentioned in subsection (1).

19 (8) The relevant chief executive may, in writing, delegate the powers  
20 and functions mentioned in subsection (9) to a person who is an  
21 SES employee or an acting SES employee in the Department.

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

24 (9) The powers and functions that may be delegated are:

25 (a) powers under Part 3 of the Regulatory Powers Act in relation  
26 to evidential material that relates to a provision mentioned in  
27 subsection (1); and

28 (b) powers and functions under the Regulatory Powers Act that  
29 are incidental to a power mentioned in paragraph (a).

30 (10) A person exercising powers or performing functions under a  
31 delegation under subsection (8) must comply with any directions of  
32 the relevant chief executive.

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1

## *Relevant court*

2

(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):

3

4

5

(a) the Federal Court of Australia;

6

(b) the Federal Circuit Court of Australia;

7

(c) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

8

9

## *Person assisting*

10

(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).

11

12

13

14

## *External Territories*

15

(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.

16

17

18

## **Division 4—Infringement notices**

19

### **49C Infringement notices**

20

#### *Provisions subject to an infringement notice*

21

(1) A civil penalty provision of this Act is subject to an infringement notice under Part 5 of the Regulatory Powers Act.

22

23

Note: Part 5 of the Regulatory Powers Act creates a framework for using infringement notices in relation to provisions.

24

25

#### *Infringement officer*

26

(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).

27

28

29

(3) The Secretary may, by writing, authorise a person who:

---

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (a) is an SES employee, or an acting SES employee, in:  
2 (i) the Department; or  
3 (ii) a relevant Commonwealth regulator; or  
4 (b) holds, or is acting in, a position in a relevant Commonwealth  
5 regulator that is equivalent to, or higher than, a position  
6 occupied by an SES employee;  
7 to be an infringement officer in relation to the provisions  
8 mentioned in subsection (1).

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

#### 11 *Relevant chief executive*

- 12 (4) For the purposes of Part 5 of the Regulatory Powers Act, the  
13 Secretary is the relevant chief executive in relation to the  
14 provisions mentioned in subsection (1).  
15 (5) The relevant chief executive may, in writing, delegate any or all of  
16 the relevant chief executive's powers and functions under Part 5 of  
17 the Regulatory Powers Act to a person who is an SES employee or  
18 an acting SES employee in the Department.

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

- 21 (6) A person exercising powers or performing functions under a  
22 delegation under subsection (5) must comply with any directions of  
23 the relevant chief executive.

#### 24 *External Territories*

- 25 (7) Part 5 of the Regulatory Powers Act, as it applies in relation to the  
26 provisions mentioned in subsection (1), extends to every external  
27 Territory.

### 28 **58 Paragraphs 51(1)(b) and (c)**

29 Repeal the paragraphs, substitute:

- 30 (b) the asset relates to a critical infrastructure sector; and  
31 (c) the Minister is satisfied that the asset is critical to:  
32 (i) the social or economic stability of Australia or its  
33 people; or
-



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

- 1 (ii) the defence of Australia; or  
2 (iii) national security; and  
3 (d) there would be a risk to:  
4 (i) the social or economic stability of Australia or its  
5 people; or  
6 (ii) the defence of Australia; or  
7 (iii) national security;  
8 if it were publically known that the asset is a critical  
9 infrastructure asset.

## 10 **59 Subsection 51(1) (note 1)**

11 Repeal the note.

## 12 **60 Subsection 51(1) (note 2)**

13 Omit “Note 2”, substitute “Note”.

## 14 **61 After subsection 51(2)**

15 Insert:

- 16 (2A) The declaration may do any or all of the following:  
17 (a) determine that Part 2 applies to the asset;  
18 (b) determine that Part 2A applies to the asset;  
19 (c) determine that Part 2B applies to the asset.

## 20 **62 Paragraph 51(3)(b)**

21 Repeal the paragraph, substitute:

- 22 (b) if the asset is a tangible asset located (wholly or partly) in a  
23 State, the Australian Capital Territory or the Northern  
24 Territory—the First Minister of the State, the Australian  
25 Capital Territory or the Northern Territory, as the case  
26 requires.

## 27 **63 Subsection 51(4)**

28 Repeal the subsection.

## 29 **64 After section 51**

30 Insert:

---

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

1 **51A Consultation—declaration**

- 2 (1) Before making a declaration under section 51 that specifies an  
3 entity as the responsible entity for an asset, the Minister must give  
4 the entity a notice:
- 5 (a) setting out the proposed declaration; and  
6 (b) inviting the entity to make submissions to the Minister about  
7 the proposed declaration within:
- 8 (i) 28 days after the notice is given; or  
9 (ii) if a shorter period is specified in the notice—that shorter  
10 period.
- 11 (2) The Minister must consider any submissions received within:
- 12 (a) the 28-day period mentioned in subparagraph (1)(b)(i); or  
13 (b) if a shorter period is specified in the notice—that shorter  
14 period.
- 15 (3) The Minister must not specify a shorter period in the notice unless  
16 the Minister is satisfied that the shorter period is necessary due to  
17 urgent circumstances.
- 18 (4) The notice must set out the reasons for making the declaration,  
19 unless the Minister is satisfied that doing so would be prejudicial to  
20 security.

21 **65 Subsection 52(5)**

22 Repeal the subsection.

23 **66 After Part 6**

24 Insert:

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 **Part 6A—Declaration of systems of national**  
2 **significance by the Minister**

3 **Division 1—Simplified outline of this Part**

4 **52A Simplified outline of this Part**

5 The Minister may privately declare a critical infrastructure asset to  
6 be a system of national significance.

7 The Minister must notify each reporting entity for an asset that is a  
8 declared system of national significance.

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

13 Note: It is an offence to disclose that an asset has been declared a system of  
14 national significance (see section 45).

15 **Division 2—Declaration of systems of national significance**  
16 **by the Minister**

17 **52B Declaration of systems of national significance by the Minister**

- 18 (1) The Minister may, in writing, declare a particular asset to be a  
19 system of national significance if:  
20 (a) the asset is a critical infrastructure asset; and  
21 (b) the Minister is satisfied that the asset is of national  
22 significance.
- 23 (2) In determining whether an asset is of national significance for the  
24 purposes of subsection (1), the Minister must have regard to:  
25 (a) if the Minister is aware of one or more interdependencies  
26 between the asset and one or more other critical infrastructure  
27 assets—the nature and extent of those interdependencies; and  
28 (b) such other matters (if any) as the Minister considers relevant.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

- 1 (3) The Minister must notify the following of the declaration, in  
2 writing, within 30 days after making the declaration in relation to  
3 an asset:
- 4 (a) each reporting entity for the asset;  
5 (b) if the asset is a tangible asset located (wholly or partly) in a  
6 State, the Australian Capital Territory or the Northern  
7 Territory—the First Minister of the State, the Australian  
8 Capital Territory or the Northern Territory, as the case  
9 requires.
- 10 (4) A declaration under subsection (1) is not a legislative instrument.
- 11 (5) To avoid doubt, an asset may be the subject of a declaration under  
12 subsection (1) even if the asset is not a system.

#### 13 **52C Consultation—declaration**

- 14 (1) Before making a declaration under section 52B in relation to an  
15 asset, the Minister must give the responsible entity for the asset a  
16 notice:
- 17 (a) setting out the proposed declaration; and  
18 (b) inviting the entity to make submissions to the Minister about  
19 the proposed declaration within:  
20 (i) 28 days after the notice is given; or  
21 (ii) if a shorter period is specified in the notice—that shorter  
22 period.
- 23 (2) The Minister must consider any submissions received within:  
24 (a) the 28-day period mentioned in subparagraph (1)(b)(i); or  
25 (b) if a shorter period is specified in the notice—that shorter  
26 period.
- 27 (3) The Minister must not specify a shorter period in the notice unless  
28 the Minister is satisfied that the shorter period is necessary due to  
29 urgent circumstances.
- 30 (4) The notice must set out the reasons for making the declaration,  
31 unless the Minister is satisfied that doing so would be prejudicial to  
32 security.

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1 **52D Notification of change to reporting entities for asset**

2 *Scope*

- 3 (1) This section applies if a reporting entity (the *first entity*) for an  
4 asset declared under subsection 52B(1) to be a system of national  
5 significance:  
6 (a) ceases to be a reporting entity for the asset; or  
7 (b) becomes aware of another reporting entity for the asset  
8 (whether or not as a result of the first entity ceasing to be a  
9 reporting entity).

10 *Notification*

- 11 (2) The first entity must, within 30 days, notify the Secretary of the  
12 following:  
13 (a) the fact in paragraph (1)(a) or (b) (as the case requires);  
14 (b) if another entity is a reporting entity for the asset—the name  
15 of each other entity and the address of each other entity’s  
16 head office or principal place of business (to the extent  
17 known by the first entity).
- 18 Civil penalty: 150 penalty units.
- 19 (3) The first entity must use the entity’s best endeavours to determine  
20 the name and relevant address of any other entity for the purposes  
21 of paragraph (2)(b).
- 22 (4) If the Secretary is notified of another entity under paragraph (2)(b),  
23 the Secretary must notify the other entity of the declaration under  
24 subsection 52B(1), in writing, within 30 days after being notified  
25 under that paragraph.

26 **67 Division 4 of Part 7 (at the end of the heading)**

27 Add “etc.”.

28 **68 Subsection 59(1)**

29 After “this Act”, insert “(other than Part 3A)”.

# EXPOSURE DRAFT

## Schedule 1 Security of critical infrastructure

### Part 1 General amendments

---

#### 69 At the end of subsection 60(2)

Add:

- ; and (f) the number of annual reports given under section 30AG during the financial year; and
- (g) the number of annual reports given under section 30AG during the financial year that included a statement to the effect that a critical infrastructure risk management program was up to date at the end of the financial year; 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
- (j) the number of notices given to entities under section 30CB during the financial year; and
- (k) the number of notices given to entities under section 30CM during the financial year; and
- (l) the number of notices given to entities under section 30CU during the financial year; and
- (m) the number of notices given to entities under Division 5 of Part 2C during the financial year; 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; and
- (r) the number of declarations of assets as systems of national significance that were made under section 52B during the financial year.

#### 70 After section 60

Insert:

---

# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
General amendments **Part 1**

---

1     **60AA Compensation for acquisition of property**

2             (1) If the operation of this Act would result in an acquisition of  
3             property (within the meaning of paragraph 51(xxxi) of the  
4             Constitution) from an entity otherwise than on just terms (within  
5             the meaning of that paragraph), the Commonwealth is liable to pay  
6             a reasonable amount of compensation to the entity.

7             (2) If the Commonwealth and the entity do not agree on the amount of  
8             the compensation, the entity may institute proceedings in:  
9                 (a) the Federal Court of Australia; or  
10                (b) the Supreme Court of a State or Territory;  
11             for the recovery from the Commonwealth of such reasonable  
12             amount of compensation as the court determines.

13     **60AB Service of notices, directions and instruments by electronic**  
14     **means**

15             Paragraphs 9(1)(d) and (2)(d) of the *Electronic Transactions Act*  
16             1999 do not apply to a notice, direction or instrument under:

- 17                 (a) this Act; or  
18                 (b) the rules; or  
19                 (c) the Regulatory Powers Act, so far as that Act relates to this  
20             Act.

21             Note:         Paragraphs 9(1)(d) and (2)(d) of the *Electronic Transactions Act 1999*  
22             deal with the consent of the recipient of information to the information  
23             being given by way of electronic communication.

# EXPOSURE DRAFT

Schedule 1 Security of critical infrastructure

Part 2 Application provisions

---

1 **Part 2—Application provisions**

2 **71 Application—subsections 9(3) and (4) of the *Security of***  
3 ***Critical Infrastructure Act 2018***

4 The amendments of subsections 9(3) and (4) of the *Security of Critical*  
5 *Infrastructure Act 2018* made by this Schedule apply in relation to rules  
6 made after the commencement of this item.

7 **72 Application—section 51 of the *Security of Critical***  
8 ***Infrastructure Act 2018***

9 The amendments of section 51 of the *Security of Critical Infrastructure*  
10 *Act 2018* made by this Schedule apply in relation to a declaration made  
11 after the commencement of this item.



# EXPOSURE DRAFT

Security of critical infrastructure **Schedule 1**  
Amendments contingent on the commencement of the Federal Circuit and Family Court  
of Australia Act 2020 **Part 3**

---

1 **Part 3—Amendments contingent on the**  
2 **commencement of the Federal Circuit and**  
3 **Family Court of Australia Act 2020**

4 *Security of Critical Infrastructure Act 2018*

5 **73 Paragraphs 49A(12)(b) and 49B(11)(b)**

6 Omit “Federal Circuit Court of Australia”, substitute “Federal Circuit  
7 and Family Court of Australia (Division 2)”.

# EXPOSURE DRAFT

Schedule 2 Australian Signals Directorate

---

1  
2

## Schedule 2—Australian Signals Directorate

3

### *Criminal Code Act 1995*

4

#### **1 Subsection 476.4(2) of the *Criminal Code***

5

Omit “section 476.5”, substitute “sections 476.5 and 476.6”.

6

#### **2 Section 476.5 of the *Criminal Code* (at the end of the heading)**

7

8

Add “—ASIS and AGO”.

9

#### **3 Subsection 476.5(1) of the *Criminal Code***

10

Omit “ASIS, AGO or ASD”, substitute “ASIS or AGO”.

11

#### **4 Subsection 476.5(3) of the *Criminal Code* (definition of *ASD*)**

12

13

Repeal the definition.

14

#### **5 Subsection 476.5(3) of the *Criminal Code* (paragraph (b) of the definition of *staff member*)**

15

16

Repeal the paragraph.

17

#### **6 At the end of Division 476 of the *Criminal Code***

18

Add:

19

#### **476.6 Liability for certain acts—ASD**

20

(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:

21

22

23

24

25

26

27

28

(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.

# EXPOSURE DRAFT

Australian Signals Directorate **Schedule 2**

---

- 1 (2) A person is not subject to any civil or criminal liability for  
2 engaging in conduct inside or outside Australia if:  
3 (a) the conduct is preparatory to, in support of, or otherwise  
4 directly connected with, overseas activities of ASD; and  
5 (b) the conduct:  
6 (i) taken together with a computer-related act, event,  
7 circumstance or result that took place, or was intended  
8 to take place, outside Australia, could amount to an  
9 offence; but  
10 (ii) in the absence of that computer-related act, event,  
11 circumstance or result, would not amount to an offence;  
12 and  
13 (c) the conduct is engaged in in the proper performance of a  
14 function of ASD.
- 15 (3) Subsection (2) is not intended to permit any conduct in relation to  
16 premises, persons, computers, things, or carriage services in  
17 Australia, being:  
18 (a) conduct which ASIO could not engage in without a Minister  
19 authorising it by warrant issued under Division 2 of Part III  
20 of the *Australian Security Intelligence Organisation Act 1979*  
21 or under Part 2-2 of the *Telecommunications (Interception*  
22 *and Access) Act 1979*; or  
23 (b) conduct engaged in to obtain information that ASIO could  
24 not obtain other than in accordance with Division 3 of  
25 Part 4-1 of the *Telecommunications (Interception and*  
26 *Access) Act 1979*.
- 27 (4) Subsections (1) and (2) have effect despite anything in a law of the  
28 Commonwealth or of a State or Territory, whether passed or made  
29 before or after the commencement of this subsection, unless the  
30 law expressly provides otherwise.
- 31 (5) Subsection (4) does not affect the operation of subsection (3).

32 *Certificate*

- 33 (6) The Inspector-General of Intelligence and Security may give a  
34 certificate in writing certifying any fact relevant to the question of  
35 whether conduct was engaged in in the proper performance of a  
36 function of ASD.
-

# EXPOSURE DRAFT

1 (7) In any proceedings, a certificate given under subsection (6) is  
2 prima facie evidence of the facts certified.

3 *Notice to Inspector-General of Intelligence and Security*

4 (8) If:

- 5 (a) a person engages in conduct referred to in subsection (1) or  
6 (2) in relation to ASD; and  
7 (b) the conduct causes material damage, material interference or  
8 material obstruction to a computer (within the meaning of  
9 section 22 of the *Australian Security Intelligence*  
10 *Organisation Act 1979*) in Australia; and  
11 (c) apart from this section, the person would commit an offence  
12 against this Part;

13 then the agency head (within the meaning of the *Intelligence*  
14 *Services Act 2001*) of ASD must, as soon as practicable, give a  
15 written notice to the Inspector-General of Intelligence and Security  
16 that:

- 17 (d) informs the Inspector-General of Intelligence and Security of  
18 that fact; and  
19 (e) provides details about the conduct that caused the damage,  
20 interference or obstruction to the computer.

21 (9) This section has effect in addition to, and does not limit, section 14  
22 of the *Intelligence Services Act 2001*.

23 *Definitions*

24 (10) In this section:

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

26 **civil or criminal liability** means any civil or criminal liability  
27 (whether under this Part, under another law or otherwise).

28 **computer-related act, event, circumstance or result** means an act,  
29 event, circumstance or result involving:

- 30 (a) the reliability, security or operation of a computer; or  
31 (b) access to, or modification of, data held in a computer or on a  
32 data storage device; or  
33 (c) electronic communication to or from a computer; or
-

# EXPOSURE DRAFT

Australian Signals Directorate **Schedule 2**

---

- 1 (d) the reliability, security or operation of any data held in or on  
2 a computer, computer disk, credit card, or other data storage  
3 device; or  
4 (e) possession or control of data held in a computer or on a data  
5 storage device; or  
6 (f) producing, supplying or obtaining data held in a computer or  
7 on a data storage device.

8 ***staff member***, in relation to ASD, means:

- 9 (a) the Director-General of ASD; or  
10 (b) a member of the staff of ASD (whether an employee of ASD,  
11 a consultant or contractor to ASD, or a person who is made  
12 available by another Commonwealth or State authority or  
13 other person to perform services for ASD).

## 14 **7 Application of amendments**

15 The amendments made by this Schedule apply in relation to conduct  
16 engaged in after the commencement of this Schedule.