



Australian Government
Department of Home Affairs

Submission

For decision

PDMS Ref. Number: MS24-001585

Date of Clearance: 30/08/2024

To Minister for Home Affairs, Minister for Immigration and Multicultural Affairs, Minister for Cyber Security

Subject Prime Minister's Approval to Release Exposure Draft - Cyber Security Legislative Reforms

Timing s. 47C(1) [REDACTED]

Recommendations

That you:

1. **agree** to the seek the Prime Minister's approval for limited release of the Exposure Draft of the entire updated Cyber Security Legislative Package – encompassing the Cyber Security Bill at **Attachment A**, Intelligence Services and Other Legislation Amendment (Cyber Security) Bill at **Attachment B** and associated explanatory material at **Attachment C**, and the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill at **Attachment D** S. 47C(1) [REDACTED]

agreed / not agreed

S. 47C(1)

signed / not signed

signed / not signed

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Minister for Home Affairs, Minister for Immigration and
Multicultural Affairs, Minister for Cyber Security

Signature.....

Date:...../...../2024

Minister's Comments

Key Issues

1. This Submission seeks **S. 47C(1)** the Prime Minister's agreement to undertake a limited release of the Exposure Drafts for the Cyber Security Legislative Package, encompassing the draft of the Cyber Security Bill (**Attachment A** refers), draft Intelligence Services and Other Legislation Amendment (Cyber Security) Bill (ISA Bill) (**Attachment B** refers), and associated explanatory material (**Attachment C** refers) and the draft of Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill (ERP Bill) (**Attachment D** refers), and associated explanatory material (**Attachment E** refers) for targeted consultation from 2 September to 6 September 2024.

2.

S. 47C(1)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 47C(1)

5. Should the Prime Minister agree to the details of the package to commence Exposure Draft consultation, the Department will undertake the steps for targeted consultation as agreed by you on 23 August 2024 (MS24-001275 refers).

Background

6. S. 47C(1)

7. On 21 August 2024, you agreed to target an introduction date for the entire Cyber Security Legislative Package of the week commencing 8 October 2024 and wrote to the Prime Minister to seek his agreement to retain category T status for these Bills, to ensure the Package can pass before the end of the Spring 2024 sitting period (MS24-001560 refers). S. 34(3)

Consultation – internal/external

8. Internal: The following have been consulted on the development of this Submission - Industry Partnerships and Infrastructure Policy Division, Cyber and Technology Security Policy Division and Legal Group. The Cyber Security Legislative Package and associated explanatory material have been consulted on with National Security Division, National Office of Cyber Security, and the Cyber and Infrastructure Security Centre.

9. S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Consultation – Secretary / Associate Secretary Immigration / ABF Commissioner

10. The Secretary, Associate Secretary and ABF Commissioner were not consulted on this submission.

Client service implications

11. Nil.

Risks and Sensitivities

12. s. 42(1)
13. Due to the nature of the legislation and compressed exposure draft consultation period, the Department recommends the Cyber Security Legislative Package be immediately referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) following introduction to Parliament. This will provide a further opportunity for public consultation on the legislative package. It will also provide an opportunity for parliamentary oversight and scrutiny, and to build bipartisan support for this important legislative package.
14. Introducing in October may reduce the time the Parliament and PJCIS have to consider the Cyber Legislative Package. This may delay passage to Autumn 2025 sittings. To mitigate this, you could provide an Exposure Draft of the Package to the PJCIS during targeted consultation with industry. The Department could also privately brief the PJCIS ahead of formal referral in October.

Financial/systems/legal/deregulation/media implications

15. s. 42(1)
16. There are no financial or systems implications considered at this time in relation to the release of the EDs of the Bills and related consultation. There are no direct media implications anticipated given that these Bills are being S. 47E(d)
- s. 47E(d)
17. s. 42(1)

Attachments

Attachment A Exposure Draft Cyber Security Bill

Attachment B Exposure Draft Intelligence Services Amendment (Cyber Security) Bill 2024

s. 7(2A)

Attachment D Exposure Draft Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill

Attachment E Explanatory document to the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill

s. 47C(1)

s. 7(2A)

s. 47E(d)

s. 47C(1)

s. 47E(d)

Authorising Officer

Cleared by:

Hamish Hansford
Deputy Secretary
Cyber and Infrastructure Security Group

Date: 30/08/2024
Mob: s. 22(1)(a)(ii)

Contact Officer Ashley Bell, Assistant Secretary, Cyber Policy and Programs Branch, Mob: s. 22(1)(a)(ii)

Through Assistant Secretary Legislation

Released by Department of Home Affairs
under the Freedom of Information Act 1982

CC

Secretary
National Cyber Security Coordinator
DS Executive
Group Manager Legal
Chief Finance Officer
FAS Cyber and Technology Security Policy Division
FAS Industry Partnerships and Infrastructure Policy Division
FAS Cyber and Infrastructure Security Centre
FAS Executive Coordination
Assistant Secretary Security, Disputes and Operations Law

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

2022-2023-2024

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

EXPOSURE DRAFT

This is a limited circulation exposure draft. It is supplied in confidence and should be given appropriate protection.

Cyber Security Bill 2024

No. , 2024

(Home Affairs)

**A Bill for an Act relating to cyber security for
Australians, and for other purposes**

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Contents

Part 1—Preliminary 1

1 Short title 1

2 Commencement 2

3 Objects..... 3

4 Simplified outline of this Act 3

5 Extraterritoriality 4

6 Act binds the Crown..... 4

7 Concurrent operation of State and Territory laws 4

8 State constitutional powers 4

9 Definitions 4

10 Meaning of *cyber security incident* 8

Part 2—Secure-by-design standards for Internet of Things devices 10

Division 1—Preliminary 10

11 Simplified outline of this Part..... 10

12 Application of this Part..... 11

Division 2—Security standards for relevant connectable products 13

13 Security standards for relevant connectable products..... 13

14 Compliance with security standard for a relevant connectable product..... 13

15 Obligation to provide and supply products with a statement of compliance with security standard 15

Division 3—Enforcement 16

16 Compliance notice 16

17 Stop notice..... 17

18 Recall notice 18

19 Public notification of failure to comply with recall notice.. 19

Division 4—Miscellaneous 21

20 Revocation and variation of notices given under this Part.. 21

21 Internal review of decision to give compliance, stop or recall notice..... 21

22 Audit of compliance with security standard and statement of compliance 22

23 Acquisition of property..... 23

Part 3—Ransomware reporting obligations	24
Division 1—Preliminary	24
24 Simplified outline of this Part.....	24
Division 2—Reporting obligations	25
25 Application of this Part.....	25
26 Obligation to report following a ransomware payment	26
27 Liability	27
Division 3—Protection of information	28
28 Ransomware payment reports may only be used or disclosed for permitted purposes.....	28
29 Limitations on secondary use and disclosure of information in ransomware payment reports.....	29
Part 4—Coordination of major cyber security incidents	31
Division 1—Preliminary	31
30 Simplified outline of this Part.....	31
Division 2—Voluntary information sharing with the National Cyber Security Coordinator	32
31 Impacted entity may voluntarily provide information to National Cyber Security Coordinator in relation to a major cyber security incident.....	32
32 Role of the National Cyber Security Coordinator.....	33
Division 3—Protection of information	33
33 Information provided in relation to a major cyber security incident may only be used or disclosed for permitted cyber security purposes	33
34 Information in relation to other cyber security incidents	35
35 Limitations on secondary use and disclosure.....	36
36 Admissibility of information voluntarily given by impacted entity.....	37
37 National Cyber Security Coordinator not compellable as witness.....	38
Division 4—Miscellaneous	39
38 Interaction with other requirements to provide information in relation to a cyber security incident	39
Part 5—Cyber Incident Review Board	40
Division 1—Preliminary	40
39 Simplified outline of this Part.....	40

Division 2—Reviews by the Board	41
40 Reviews by the Board.....	41
41 Board may discontinue a review.....	42
42 Board may request information or documents.....	42
43 Board may require certain entities to produce documents ..	43
44 Civil penalty—failing to comply with a notice to produce documents.....	44
45 Draft review reports.....	44
46 Final review reports.....	45
47 Certain information must be redacted from final review reports.....	46
48 Protected review reports	47
Division 3—Protection of information relating to reviews	49
Subdivision A—Protection of information requested or required by the Board	49
49 Limitations on use and disclosure by the Board	49
50 Limitations on secondary use and disclosure.....	49
51 Admissibility of information voluntarily given to the Board.....	51
Subdivision B—Protection of reports	52
52 Disclosure of draft review reports prohibited	52
53 Disclosure of protected review reports prohibited.....	52
Division 4—Establishment, functions and powers of the Board	54
54 Cyber Incident Review Board	54
55 Constitution of the Board	54
56 Functions of the Board	54
57 Independence.....	55
Division 5—Terms and conditions of appointment of Board members	56
58 Appointment of Board members	56
59 Acting Chair	56
60 Terms and conditions etc. for members.....	56
Division 6—Expert Panel, staff assisting and consultants	58
61 Expert Panel	58
62 Arrangements relating to staff of the Department	58
63 Consultants	59
Division 7—Other matters relating to the Board	60
64 Board procedures.....	60

65	Liability	60
66	Certification of involvement in review	61
67	Annual report.....	61
Part 6—Regulatory powers		63
Division 1—Preliminary		63
68	Simplified outline of this Part.....	63
Division 2—Civil penalty provisions, enforceable undertakings and injunctions		64
69	Civil penalty provisions, enforceable undertakings and injunctions	64
Division 3—Monitoring and investigation powers		67
70	Monitoring powers	67
71	Investigation powers.....	69
Division 4—Infringement notices		71
72	Infringement notices	71
Division 5—Other matters		73
73	Contravening a civil penalty provision	73
Part 7—Miscellaneous		74
74	Simplified outline of this Part.....	74
75	How this Act applies in relation to non-legal persons	74
76	Delegation by Secretary.....	75
77	Rules.....	76

1 **A Bill for an Act relating to cyber security for**
2 **Australians, and for other purposes**

3 The Parliament of Australia enacts:

4 **Part 1—Preliminary**
5

6 **1 Short title**

7 This Act is the *Cyber Security Act 2024*.

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

Part 1 Preliminary

Section 2

2 Commencement

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

Commencement information		
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. Part 1 and anything in this Act not elsewhere covered by this table	The day after this Act receives the Royal Assent.	
2. Part 2	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 12 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	
3. Part 3	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.	
4. Part 4	The day after this Act receives the Royal Assent.	
5. Part 5	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.	
6. Parts 6 and 7	The day after this Act receives the Royal Assent.	

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

- (a) improve the cyber security of products that can connect directly or indirectly to the internet that are supplied in Australia; and
- (b) encourage the provision of information to the Australian Government to assist the response to cyber security incidents.

The Cyber Incident Review Board is established by this Act. Its functions are to undertake reviews of cyber security incidents and make recommendations to Government and industry about actions that could be taken to prevent, detect, respond to or minimise the impact of, incidents of a similar nature in the future.

Part 1 Preliminary

Section 5

1 **5 Extraterritoriality**

2 This Act applies both within and outside Australia.

3 Note: This Act extends to every external Territory.

4 **6 Act binds the Crown**

5 (1) This Act binds the Crown in each of its capacities.

6 (2) This Act does not make the Crown liable to be prosecuted for an
7 offence.

8 Note: The Crown (other than a Crown authority) is not liable to a pecuniary
9 penalty for the breach of a civil penalty provision or to be given an
10 infringement notice: see subsections 69(7) and 72(7).

11 (3) The protection in subsection (2) does not apply to an authority of
12 the Crown.

13 **7 Concurrent operation of State and Territory laws**

14 This Act is not intended to exclude or limit the operation of a law
15 of a State or Territory to the extent that that law is capable of
16 operating concurrently with this Act.

17 **8 State constitutional powers**

18 This Act does not enable a power to be exercised to the extent that
19 it would impair the capacity of a State to exercise its constitutional
20 powers.

21 **9 Definitions**

22 In this Act:

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

24 **benefit** includes any advantage and is not limited to property.

25 **Board member** means a member of the Board, and includes the
26 Chair.

- 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
- business** has the same meaning as in the *Income Tax Assessment Act 1997*.
- Chair** means the Chair of the Cyber Incident Review Board.
- civil penalty provision** has the same meaning as in the Regulatory Powers Act.
- Commonwealth body** means:
- (a) a Minister of the Commonwealth; or
 - (b) a Department of State of the Commonwealth; or
 - (c) a body (whether incorporated or not) that is:
 - (i) established, or continued in existence, for a public purpose by or under a law of the Commonwealth; and
 - (ii) entitled to the immunities and privileges of the Crown in right of the Commonwealth.
- Commonwealth enforcement body** means:
- (a) the agency known as the Australian Criminal Intelligence Commission established by the *Australian Crime Commission Act 2002*; or
 - (b) the Australian Federal Police; or
 - (c) the Australian Prudential Regulation Authority; or
 - (d) the Australian Securities and Investments Commission; or
 - (e) the Inspector of the National Anti-Corruption Commission; or
 - (f) the Office of the Director of Public Prosecutions; or
 - (g) the National Anti-Corruption Commissioner; or
 - (h) Sport Integrity Australia; or
 - (i) another Commonwealth body, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction for a criminal offence.
- Commonwealth officer** has the same meaning as in Part 5.6 of the *Criminal Code*.

Part 1 Preliminary

Section 9

- 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
- computer** has the same meaning as in the *Security of Critical Infrastructure Act 2018*.
- coronial inquiry** means a coronial inquiry, coronial investigation or coronial inquest under a law of the Commonwealth, or of a State or Territory.
- critical infrastructure asset** has the same meaning as in the *Security of Critical Infrastructure Act 2018*.
- Cyber Incident Review Board** or **Board** means the Cyber Incident Review Board established by section 54.
- cyber security incident** has the meaning given by section 10.
- designated Commonwealth body** means:
- (a) a Department, or a body established by a law of the Commonwealth, specified in the rules; or

(b) if no rules are made for the purposes of paragraph (a)—the Department and ASD.
- draft review report** has the meaning given by subsection 45(2).
- entity** means any of the following:
- (a) an individual;

(b) a body corporate;

(c) a partnership;

(d) an unincorporated association that has a governing body;

(e) a trust;

(f) an entity that is a responsible entity for a critical infrastructure asset to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies.
- Expert Panel** means the Expert Panel established by the Board under section 61.
- final review report** has the meaning given by subsection 46(1).
- intelligence agency** means:
- (a) the Australian Geospatial-Intelligence Organisation; or

Section 9

- 1
- (b) the Australian Secret Intelligence Service; or
- 2
- (c) the Australian Security Intelligence Organisation; or
- 3
- (d) ASD; or
- 4
- (e) the Defence Intelligence Organisation; or
- 5
- (f) the Office of National Intelligence.
- 6
- internet-connectable product** has the meaning given by subsection
- 7
- 12(4).
- 8
- major cyber security incident** has the meaning given by subsection
- 9
- 31(3).
- 10
- manufacturer** has the same meaning as in the Australian
- 11
- Consumer Law.
- 12
- National Cyber Security Coordinator** means:
- 13
- (a) the officer of the Department known as the National Cyber
- 14
- Security Coordinator; and
- 15
- (b) the APS employees, and officers or employees of
- 16
- Commonwealth bodies, whose services are made available to
- 17
- the officer in connection with the performance of any of the
- 18
- officer’s functions or the exercise of any of the officer’s
- 19
- powers under this Act.
- 20
- network-connectable product** has the meaning given by subsection
- 21
- 12(5).
- 22
- permitted cyber security purposes** has the meaning given by
- 23
- subsection 33(3).
- 24
- personal information** has the same meaning as in the *Privacy Act*
- 25
1988.
- 26
- protected review report** has the meaning given by subsection 47(2).
- 27
- ransomware payment** has the meaning given by subsection 25(1).
- 28
- ransomware payment report** means a report given by an entity
- 29
- under subsection 26(1).

Part 1 Preliminary

Section 10

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- Regulatory Powers Act** means the *Regulatory Powers (Standard Provisions) Act 2014*.
- relevant connectable product** has the meaning given by subsection 12(2).
- reporting business entity** has the meaning given by subsection 25(2).
- responsible entity**, for an asset, has the same meaning as in the *Security of Critical Infrastructure Act 2018*.
- review report** has the meaning given by subsection 46(1).
- Secretary** means the Secretary of the Department.
- sensitive information** has the same meaning as in the *Privacy Act 1988*.
- sensitive review information** has the meaning given by subsection 47(2).
- State body** means:
- (a) a Minister of a State or Territory; or

(b) a Department of State of a State or Territory or a Department of the Public Service of a State or Territory; or

(c) a body (whether incorporated or not) that is:

(i) established, or continued in existence, for a public purpose by or under a law of a State or Territory; and

(ii) entitled to the immunities and privileges of the Crown in right of the State or Territory.
- supply** has the same meaning as in the Australian Consumer Law.

10 Meaning of cyber security incident

- 25
- 26
- 27
- 28
- 29
- (1) A **cyber security incident** is one or more acts, events or circumstances:
- (a) of a kind covered by the meaning of **cyber security incident** in the *Security of Critical Infrastructure Act 2018*; or

Section 10

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- (b) involving unauthorised impairment of electronic communication to or from a computer, within the meaning of that phrase in that Act, but including mere interception of any such communication.
- (2) However, an incident is only a *cyber security incident* for the purposes of this Act if:
- (a) the incident involves a critical infrastructure asset; or
- (b) the incident involves the activities of an entity that is a corporation to which paragraph 51(xx) of the Constitution applies; or
- (c) the incident is, was or would probably be effected by means of a telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution (including, for example, by means of the internet); or
- (d) the incident is impeding or impairing, has impeded or impaired or would probably impede or impair the ability of a computer to connect to such a service.

Part 2 Secure-by-design standards for Internet of Things devices
Division 1 Preliminary

Section 11

Part 2—Secure-by-design standards for Internet of Things devices

Division 1—Preliminary

11 Simplified outline of this Part

The rules may provide mandatory security standards for products that can directly or indirectly connect to the internet (called relevant connectable products) that will be acquired in Australia in specified circumstances.

If the rules provide a security standard for a product:

- (a) manufacturers must manufacture the product in compliance with the requirements of the security standard if they are aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in the specified circumstances; and
- (b) those manufacturers must also comply with any other obligations relating to the product in the security standard (for example, obligations to publish information about the product); and
- (c) if the product does not comply it must not be supplied in Australia if the supplier is aware, or could reasonably be expected to be aware, that the products will be acquired in Australia in those specified circumstances; and
- (d) those suppliers must supply the product in Australia accompanied by a statement of compliance provided by the manufacturer of the product.

A compliance notice, a stop notice and a recall notice may be given for non-compliance with obligations in this Part. Internal review may be sought for a decision to issue a notice.

An independent audit of a product may be undertaken to determine compliance with the requirements of a security standard or

requirements for the statement of compliance. The Secretary may request the manufacturer or supplier to provide the product, the statement of compliance or both for the purposes of the audit.

12 Application of this Part

- (1) This Part applies to a relevant connectable product that is manufactured or supplied on or after the commencement of this Part.
- (2) A **relevant connectable product** is a product that:
 - (a) is an internet-connectable product or a network-connectable product; and
 - (b) is not exempted under the rules.
- (3) For the purposes of paragraph (2)(b), the rules may specify that:
 - (a) classes of products are exempted; or
 - (b) particular products are exempted.
- (4) An **internet-connectable product** is a product that is capable of connecting to the internet using a communication protocol that forms part of the internet protocol suite to send and receive data over the internet.
- (5) A **network-connectable product** is a product that:
 - (a) is capable of both sending and receiving data by means of a transmission involving electrical or electromagnetic energy; and
 - (b) is not an internet-connectable product; and
 - (c) meets the condition in subsection (6) or (7).
- (6) A product meets the condition in this subsection if it is capable of connecting directly to an internet-connectable product by means of a communication protocol that forms part of the internet protocol suite.
- (7) Subject to subsections (8) and (9), a product meets the condition in this subsection if:

Part 2 Secure-by-design standards for Internet of Things devices**Division 1** PreliminarySection 12

- 1 (a) it is capable of connecting directly to 2 or more products at
2 the same time by means of a communication protocol that
3 does not form part of the internet protocol suite; and
4 (b) it is capable of connecting directly to an internet-connectable
5 product by means of such a communication protocol
6 (whether or not at the same time as it connects to any other
7 product).
- 8 (8) A product consisting of a wire or cable that is used merely to
9 connect the product to another product does not meet the condition
10 in subsection (7).
- 11 (9) If:
12 (a) two or more products are designed to be used together for the
13 purposes of facilitating the use of a computer; and
14 (b) at least one of the products (the **linking product**) is capable
15 of connecting directly to an internet-connectable product
16 (whether the computer or some other product) by means of a
17 communication protocol that does not form part of the
18 internet protocol suite; and
19 (c) each of the products (the **input products**) that is not a linking
20 product is capable of connecting directly to the linking
21 product, or, if there is more than one linking product, to each
22 linking product:
23 (i) wirelessly; and
24 (ii) by means of a communication protocol that does not
25 form part of the internet protocol suite;
26 each of the input products meets the condition in subsection (7).
- 27 (10) For the purposes of subsections (4) to (9), a product is not
28 prevented from being regarded as connecting directly to another
29 product merely because the connection involves the use of a wire
30 or cable.

1 **Division 2—Security standards for relevant connectable**
2 **products**

3 **13 Security standards for relevant connectable products**

- 4 (1) The rules may make provision for, or in relation to, security
5 standards for specified classes of relevant connectable products
6 that will be acquired in Australia in specified circumstances.
- 7 (2) Without limiting subsection (1) a class of relevant connectable
8 products specified for the purposes of that subsection may consist
9 of a particular relevant connectable product or of all relevant
10 connectable products.
- 11 (3) Despite subsection 14(2) of the *Legislation Act 2003*, the rules may
12 make provision in relation to a matter by applying, adopting or
13 incorporating, with or without modification, any matter contained
14 in an instrument or other writing as in force or existing from time
15 to time.

16 **14 Compliance with security standard for a relevant connectable**
17 **product**

18 *Manufacturer must comply*

- 19 (1) An entity must manufacture a relevant connectable product in
20 compliance with the requirements of the security standard for a
21 class of relevant connectable product that will be acquired in
22 Australia in specified circumstances if:
- 23 (a) the product is included in that class; and
24 (b) the entity is aware, or could reasonably be expected to be
25 aware, that the product will be acquired in Australia in those
26 circumstances.
- 27 (2) The entity must comply with any other requirements of the security
28 standard that apply to the manufacturer of a product included in
29 that class.

Part 2 Secure-by-design standards for Internet of Things devices
Division 2 Security standards for relevant connectable products

Section 14

- 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
- 32
- (3) An entity must not supply a product in Australia that was not manufactured in compliance with the requirements of the security standard for a class of relevant connectable product that will be acquired in Australia in specified circumstances if:
 - (a) the product is included in that class; and
 - (b) the entity is aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in those circumstances.
 - (4) The entity must comply with any other requirements of the security standard that apply to the supplier of a product included in that class.
- Exception*
- (5) However, to the extent that a requirement in the security standard does not relate to any of the matters in subsection (6), an entity is not required to comply with subsections (1) to (4) if the entity is not:
 - (a) an entity that is a corporation to which paragraph 51(xx) of the Constitution applies; or
 - (b) an entity that is undertaking activities in the course of, or in relation to, trade or commerce with other countries, among the States, between Territories or between a Territory and a State.
 - (6) The matters are the following:
 - (a) the direct, or indirect, connection of the relevant connectable product to, a telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution (including, for example, connection to the internet);
 - (b) the direct, or indirect, use by the relevant connectable product of such a service (including, for example, use of the internet);
 - (c) measures that would protect the relevant connectable product from an attack effected by means of such a service (including, for example, by means of the internet).

15 **Obligation to provide and supply products with a statement of compliance with security standard**

Manufacturer must provide statement of compliance

- (1) An entity that manufactures a relevant connectable product must provide, for the supply of the product in Australia, a statement of compliance with the security standard for a class of relevant connectable product that will be acquired in Australia in specified circumstances if:
 - (a) the product is included in that class; and
 - (b) the entity is aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in those circumstances.
- (2) The entity must retain a copy of the statement of compliance for the period specified in the rules.

Supplier must supply the product with statement of compliance provided by manufacturer

- (3) An entity that supplies a relevant connectable product in Australia must supply the product with a statement of compliance with the security standard for a class of relevant connectable product that will be acquired in Australia in specified circumstances if:
 - (a) the product is included in that class; and
 - (b) the entity is aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in those circumstances.
- (4) The entity must retain a copy of the statement of compliance for the period specified in the rules.

Requirements for statement of compliance

- (5) The statement of compliance with the security standard under subsection (1) or (2) must:
 - (a) meet the requirements provided by the rules; and
 - (b) be in the form (if any) provided by the rules.

Part 2 Secure-by-design standards for Internet of Things devices
Division 3 Enforcement

Section 16

Division 3—Enforcement

16 Compliance notice

- (1) The Secretary may give an entity that must comply with an obligation under section 14 or 15 a compliance notice if the Secretary:
- (a) is reasonably satisfied that the entity is not complying with the obligation; or
 - (b) is aware of information that suggests that the entity may not be complying with the obligation.
- (2) The compliance notice must:
- (a) set out the name of the entity to which the notice is given; and
 - (b) set out brief details of the non-compliance or possible non-compliance; and
 - (c) specify action within the entity’s control that the entity must take in order to address the non-compliance or possible non-compliance; and
 - (d) specify a reasonable period within which the entity must take the specified action; and
 - (e) if the Secretary considers it appropriate—specify a reasonable period within which the entity must provide the Secretary with evidence that the entity has taken the specified action; and
 - (f) explain what may happen if the entity does not comply with the notice; and
 - (g) explain how the entity may seek review of the decision to issue the notice; and
 - (h) set out any other matters prescribed by the rules.
- (3) Before giving the notice to the entity, the Secretary must:
- (a) notify the entity that the Secretary intends to give the notice to the entity; and

Section 17

- 1 (b) give the entity a specified period (which must not be shorter
2 than 10 days) to make representations about the giving of the
3 notice.
- 4 (4) Only one compliance notice may be given to an entity in relation to
5 a particular instance of the entity's non-compliance, or possible
6 non-compliance, with an obligation under section 14 or 15.

17 Stop notice

- 8 (1) The Secretary may give an entity that must comply with an
9 obligation under section 14 or 15 a stop notice if:
10 (a) the entity has been given a compliance notice under section
11 16 in relation to the non-compliance with the obligation; and
12 (b) the Secretary is reasonably satisfied that:
13 (i) the entity has not complied with the compliance notice;
14 or
15 (ii) actions taken by the entity to rectify non-compliance
16 with the obligation (whether in accordance with the
17 compliance notice or otherwise) are inadequate to
18 rectify the non-compliance.
- 19 (2) The stop notice must:
20 (a) set out the name of the entity to which the notice is given;
21 and
22 (b) set out brief details of the non-compliance; and
23 (c) specify action within the entity's control that the entity must
24 take, or refrain from taking, in order to address the
25 non-compliance; and
26 (d) specify a reasonable period within which the entity must take
27 the specified action or refrain from taking the specified
28 action; and
29 (e) if the Secretary considers it appropriate—specify a
30 reasonable period within which the entity must provide the
31 Secretary with evidence that the entity has taken the specified
32 action or refrained from taking the specified action; and
33 (f) explain what may happen if the entity does not comply with
34 the notice; and

Part 2 Secure-by-design standards for Internet of Things devices

Division 3 Enforcement

Section 18

- 1 (g) explain how the entity may seek review of the decision to
- 2 issue the notice; and
- 3 (h) set out any other matters prescribed by the rules.
- 4 (3) Before giving the notice to the entity, the Secretary must:
- 5 (a) notify the entity that the Secretary intends to give the notice
- 6 to the entity; and
- 7 (b) give the entity a specified period (which must not be shorter
- 8 than 10 days) to make representations about the giving of the
- 9 notice.
- 10 (4) Only one stop notice may be given to an entity in relation to a
- 11 particular instance of the entity's non-compliance with an
- 12 obligation under section 14 or 15.

18 Recall notice

- 14 (1) The Secretary may give an entity that must comply with an
- 15 obligation under section 14 or 15 a recall notice if:
- 16 (a) the entity has been given a stop notice under section 17 in
- 17 relation to the non-compliance with the obligation; and
- 18 (b) the Secretary is reasonably satisfied that:
- 19 (i) the entity has not complied with the stop notice; and
- 20 (ii) actions taken by the entity to rectify the non-compliance
- 21 with the obligation (whether in accordance with the
- 22 compliance notice or otherwise) are inadequate to
- 23 rectify the non-compliance.
- 24 (2) The recall notice must:
- 25 (a) set out the name of the entity to which the notice is given;
- 26 and
- 27 (b) set out brief details of the non-compliance; and
- 28 (c) specify action that the entity must take to do any or all of the
- 29 following:
- 30 (i) ensure, to the extent within the entity's control, the
- 31 product is not acquired in Australia;

- 19

Part 2 Secure-by-design standards for Internet of Things devices
Division 3 Enforcement

Section 19

- 1 (d) risks posed by the product relating to the non-compliance;
- 2 (e) any other matters prescribed by the rules.

Division 4—Miscellaneous**20 Revocation and variation of notices given under this Part**

- (1) The Secretary may, by notice in writing given to an entity, vary a compliance notice, stop notice or recall notice given under this Part to the entity.
- (2) A varied compliance notice, stop notice or recall notice has the same effect as the original notice for the purposes of this Part.
- (3) The Secretary may, by notice in writing given to an entity, revoke a compliance notice, stop notice or recall notice given under this Part to the entity if the Secretary is satisfied that the notice is no longer necessary or desirable.
- (4) If a compliance notice, stop notice or recall notice, relating to non-compliance or possible non-compliance by an entity with an obligation, is revoked under subsection (3), no further notices may be issued under this Part in relation to the non-compliance.

21 Internal review of decision to give compliance, stop or recall notice

- (1) An entity may apply, in writing, to the Secretary for review (an **internal review**) of a decision:
 - (a) to give the entity a compliance notice under section 16; or
 - (b) to give the entity a stop notice under section 17; or
 - (c) to give the entity a recall notice under section 18; or
 - (d) to vary, under section 20, a notice given to the entity.
- (2) An application for an internal review must be made within 30 days after the day on which the notice was given to the entity.
- (3) The decision maker for the internal review is:
 - (a) the Secretary; or
 - (b) if the Secretary made the decision personally—a person:
 - (i) to whom the power to issue a notice of that kind has been delegated under section 76; and

Part 2 Secure-by-design standards for Internet of Things devices**Division 4** Miscellaneous**Section 22**

- 1 (ii) that was not involved in the making of the Secretary's
2 decision.
- 3 (4) Within 30 days after the application is received, the decision-maker
4 must:
- 5 (a) review the decision; and
6 (b) affirm, vary or revoke the decision; and
7 (c) if the decision is revoked—make such other decision (if any)
8 that the decision-maker thinks appropriate.
- 9 (5) The decision-maker for the reviewable decision must, as soon as
10 practicable after making a decision under subsection (4), give the
11 applicant a written statement of the decision-maker's reasons for
12 the decision.

22 Audit of compliance with security standard and statement of compliance

- 13
14
- 15 (1) If an entity must comply with an obligation in section 14 or 15 in
16 relation to a relevant connectable product, the Secretary may
17 engage an appropriately qualified and experienced expert to carry
18 out an independent audit of the product to determine either or both
19 of the following:
- 20 (a) whether the product complies with the security standard for
21 the class of relevant connectable product;
22 (b) whether the statement of compliance for the product
23 complies with the requirements of section 15.
- 24 (2) The expert may examine the product, for example, by doing any of
25 the following:
- 26 (a) opening any package in which the product is contained;
27 (b) operating the product;
28 (c) testing or analysing the product, including through the use of
29 electronic equipment;
30 (d) if the product contains a record or document—reading the
31 record or document either directly or with the use of an
32 electronic device;
33 (e) taking photographs or video recordings of the product.

Request for product and statement of compliance

- (3) For the purposes of the examination, the Secretary may request, by notice in writing, the entity to provide the product, or the statement of compliance for the product, or both.
- (4) The notice must:
- (a) specify the product; and
 - (b) if the entity is not the manufacturer—specify the manufacturer of the product; and
 - (c) specify a reasonable period within which the entity must provide the notice; and
 - (d) specify the period for which the product will be retained for testing; and
 - (e) specify the requirements of the security standard that the product will be tested against; and
 - (f) explain the kind of testing or analysis that will be done; and
 - (g) explain what may happen if:
 - (i) the entity does not comply with the notice; or
 - (ii) the entity does not comply with its obligations in section 14 or 15 in relation to the product; and
 - (h) set out any other matters prescribed by the rules.

Compensation

- (5) An entity is entitled to be paid by the Commonwealth reasonable compensation for complying with a request under subsection (3).

23 Acquisition of property

This Part has no effect to the extent (if any) that its operation would result in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from a person otherwise than on just terms (within the meaning of that paragraph).

Part 3 Ransomware reporting obligations
Division 1 Preliminary

Section 24

- 1 **Part 3—Ransomware reporting obligations**
- 2 **Division 1—Preliminary**
- 3 **24 Simplified outline of this Part**

Certain entities must report payments or benefits (called ransomware payments) provided to an entity that is seeking to benefit from a cyber security incident.

Division 2—Reporting obligations

25 Application of this Part

- (1) This Part applies if:
- (a) a cyber security incident has occurred, is occurring or is imminent; and
 - (b) the incident has had, is having, or is likely to have, a direct or indirect impact on a reporting business entity; and
 - (c) an entity (the **extorting entity**) makes a demand of the reporting business entity, or any other entity, in order to benefit from the incident or the impact on the reporting business entity; and
 - (d) the reporting business entity provides, or is aware that another entity has provided, a payment or benefit (a **ransomware payment**) to the extorting entity that is directly related to the demand.
- (2) An entity is a **reporting business entity** if, at the time the ransomware payment is made:
- (a) the entity:
 - (i) is carrying on a business in Australia with an annual turnover for the previous financial year that exceeds the turnover threshold for that year; and
 - (ii) is not a State body; or
 - (b) the entity is a responsible entity for a critical infrastructure asset to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies.
- (3) For the purposes of subparagraph (2)(a)(i), the **turnover threshold** is:
- (a) if a business has been carried on for only part of the previous financial year—the amount worked out in the manner prescribed by the rules; or
 - (b) in any other case—the amount prescribed by, or worked out in the manner prescribed by, the rules.

Part 3 Ransomware reporting obligations**Division 2** Reporting obligationsSection 26

26 Obligation to report following a ransomware payment

- (1) The reporting business entity must give the designated Commonwealth body a report (a **ransomware payment report**) that complies with the requirements of this section within 72 hours of making the ransomware payment or becoming aware that the ransomware payment has been made (whichever is applicable).

Note: For the definition of **designated Commonwealth body**: see section 9.

- (2) The ransomware payment report must contain the following information that, at the time of making the report, the reporting business entity knows or is able, by reasonable search or enquiry, to find out:

- (a) details of the following, in accordance with any requirements prescribed by the rules:

- (i) if the reporting business entity made the payment—the reporting business entity’s contact and business details;
- (ii) if another entity made the payment—that entity’s contact and business details;
- (iii) the cyber security incident;
- (iv) the demand made by the extorting entity;
- (v) the ransomware payment;
- (vi) communications with the extorting entity relating to the incident, the demand and the payment;

- (b) such other information (if any) prescribed by the rules.

- (3) The reporting business entity may include other information in the ransomware payment report.

- (4) The ransomware payment report must be given in the manner and form (if any) prescribed by the rules.

- (5) An entity is liable to a civil penalty if the entity contravenes subsection (1).

Civil penalty: 50 penalty units.

- (6) Subsection 93(2) of the Regulatory Powers Act does not apply in relation to a contravention of subsection (1) of this section.

1
2
3
4
5
6
7
8
9
10
11

27 Liability

- (1) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with section 26.
- (2) An officer, employee or agent of an entity is not liable to an action for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1).
- (3) An entity that wishes to rely on subsection (1) in relation to an action or other proceeding bears an evidential burden (within the meaning of the Regulatory Powers Act) in relation to that matter.

Part 3 Ransomware reporting obligations**Division 3** Protection of informationSection 28

Division 3—Protection of information**28 Ransomware payment reports may only be used or disclosed for permitted purposes**

- (1) A designated Commonwealth body may only make a record of, use or disclose information provided in a ransomware payment report if making the record of, using or disclosing the information is:
- (a) for the purposes of performing functions or exercising powers under this Part or Part 6 as it applies to this Part; or
 - (b) for the purposes of proceedings under, or arising out of, section 137.1 or 137.2 of the *Criminal Code* (false and misleading information and documents) that relate to this Act; or
 - (c) for the purposes of proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act; or
 - (d) for a permitted cyber security purpose.

Note: For **permitted cyber security purposes**: see subsection 33(3).

- (2) Subsection (1) does not prohibit the recording, use or disclosure of the following information:
- (a) information that has been provided to the designated Commonwealth body by, or on behalf of, the entity to the Commonwealth to comply with:
 - (i) a requirement in Part 2B of the *Security of Critical Infrastructure Act 2018*; or
 - (ii) a requirement under the *Telecommunications Act 1997*; or
 - (iii) a requirement under a law prescribed by the rules;
 - (b) information that has already been lawfully made available to the public.

**29 Limitations on secondary use and disclosure of information in
ransomware payment reports**

- (1) An entity or a Commonwealth body who obtains information under subsection 28(1), or this section, may only make a record of, use or disclose the information for a purpose that is any of the following:
- (a) the purposes of performing functions or exercising powers under this Part or Part 6 as it applies to this Part;
 - (b) the purposes of proceedings under, or arising out of, section 137.1 or 137.2 of the *Criminal Code* (false and misleading information and documents) that relate to this Act;
 - (c) the purposes of proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act;
 - (d) a permitted cyber security purpose;
 - (e) for an intelligence agency—the purposes of its functions;
 - (f) for a Commonwealth enforcement body—the purposes of its functions relating to the investigation or enforcement of a criminal offence.
- (2) Subsection (1) does not prohibit the recording, use or disclosure of the following information:
- (a) information referred to in subsection 28(2);
 - (b) if the entity is an individual—personal information about the individual;
 - (c) if the entity is the reporting business entity that originally provided the information under section 26—the reporting business entity's own information.
- (3) An entity is liable to a civil penalty if:
- (a) the entity contravenes subsection (1); and
 - (b) the entity is not:
 - (i) a Commonwealth officer; or
 - (ii) an officer or employee of a State body; and
 - (c) any of the following applies:

Part 3 Ransomware reporting obligations
Division 3 Protection of information

Section 29

- 1
- (i) the information is sensitive information about a person
- 2
- and the person has not consented to the record, use or
- 3
- disclosure of the information;
- 4
- (ii) the information is confidential or commercially
- 5
- sensitive;
- 6
- (iii) the record, use or disclosure of the information would,
- 7
- or could reasonably be expected to, cause damage to the
- 8
- security, defence or international relations of the
- 9
- Commonwealth.
- 10
- Note 1: See the *Criminal Code* for offences for Commonwealth officers.
- 11
- Note 2: This Act does not make the Crown (other than an authority of the
- 12
- Crown) liable to a civil penalty.
- 13
- Civil penalty: 50 penalty units.

1 **Part 4—Coordination of major cyber security**
2 **incidents**

3 **Division 1—Preliminary**

4 **30 Simplified outline of this Part**

5 Information may be voluntarily provided to the National Cyber
6 Security Coordinator in relation to major cyber security incidents
7 or potential major cyber security incidents.

8 The National Cyber Security Coordinator’s role is to lead across
9 the whole of Government the coordination and triaging of action in
10 response to a major cyber security incident.

11 Information voluntarily provided under this Part may only be
12 recorded, used and disclosed for limited purposes.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Part 4 Coordination of major cyber security incidents
Division 2 Voluntary information sharing with the National Cyber Security Coordinator

Section 31

Division 2—Voluntary information sharing with the National Cyber Security Coordinator

31 Impacted entity may voluntarily provide information to National Cyber Security Coordinator in relation to a major cyber security incident

- (1) An entity (the *impacted entity*), or another entity acting on behalf of the impacted entity, may provide information to the National Cyber Security Coordinator if:
- (a) a major cyber security incident has occurred, is occurring or is imminent or a major cyber security incident may potentially occur; and
 - (b) the incident has had, is having, or is likely to have, a direct or indirect impact on the impacted entity or the impacted entity would likely be impacted by the potential incident; and
 - (c) the impacted entity is:
 - (i) carrying on a business in Australia; or
 - (ii) a responsible entity for a critical infrastructure asset to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies.

Note: For information provided in relation to other kinds of cyber security incidents: see section 34.

- (2) The information may be provided:
- (a) at any time during the response to the incident or potential incident; and
 - (b) on the entity’s own initiative or in response to a request by the National Cyber Security Coordinator.

Note: There is no obligation on the entity to provide information in response to a request.

Meaning of *major cyber security incident*

- (3) A cyber security incident is a *major cyber security incident* if:

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- (a) there is a material risk that the incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice:
- (i) the social or economic stability of Australia or its people; or
- (ii) the defence of Australia; or
- (iii) national security; or
- (b) the incident is, or is likely to be, of serious concern to the Australian people.

10

32 Role of the National Cyber Security Coordinator

- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- The role of the National Cyber Security Coordinator includes, but is not limited to, the following:
- (a) to lead across the whole of Government the coordination and triaging of action in response to a major cyber security incident;
- (b) to inform and advise the Minister and the whole of Government in relation to the whole of Government response to a major cyber security incident.

19

Division 3—Protection of information

20

21

22

33 Information provided in relation to a major cyber security incident may only be used or disclosed for permitted cyber security purposes

- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- (1) The National Cyber Security Coordinator may only make a record of, use or disclose information provided under section 31 by, or on behalf of, an entity (the *impacted entity*) in relation to a major cyber security incident or potential major cyber security incident if making the record of, using or disclosing the information is for a permitted cyber security purpose.
- (2) Subsection (1) does not prohibit the recording, use or disclosure of the following information:

Part 4 Coordination of major cyber security incidents
Division 3 Protection of information

Section 33

- (a) information that has been provided by, or on behalf of, the impacted entity to the Commonwealth about the cyber security incident to comply with:
 - (i) a requirement in Part 3 of this Act; or
 - (ii) a requirement in Part 2B of the *Security of Critical Infrastructure Act 2018*; or
 - (iii) a requirement under the *Telecommunications Act 1997*; or
 - (iv) a requirement under a law prescribed by the rules;
- (b) information that has been provided voluntarily to the National Cyber Security Coordinator by, or on behalf of, the impacted entity, other than under this Part;
- (c) information that has already been lawfully made available to the public.

Permitted cyber security purposes

- (3) The following are **permitted cyber security purposes**:
 - (a) assisting the impacted entity, and other entities acting on behalf of the impacted entity, to respond to, mitigate or resolve the cyber security incident;
 - (b) coordinating the whole of Government response to the cyber security incident;
 - (c) informing and advising the Minister, and other Ministers of the Commonwealth, about the whole of Government response to the cyber security incident;
 - (d) preventing or mitigating material risks that the cyber security incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice:
 - (i) the social or economic stability of Australia or its people; or
 - (ii) the defence of Australia; or
 - (iii) national security;
 - (e) preventing or mitigating material risks to a critical infrastructure asset to which the *Security of Critical Infrastructure Act 2018* applies;

Section 34

- 1 (f) disclosing information to ASD for the purposes of its
2 functions;
3 (h) disclosing information to:
4 (i) any other intelligence agency for the purposes of its
5 functions; or
6 (ii) a Commonwealth enforcement body for the purposes of
7 its functions relating to the investigation or enforcement
8 of a criminal offence;
9 (i) preventing or lessening a serious threat to the life or health of
10 an individual or a group of individuals.

11 **34 Information in relation to other cyber security incidents**

- 12 (1) If:
13 (a) an entity (the **impacted entity**) provides information to the
14 National Cyber Security Coordinator in relation to a cyber
15 security incident or a cyber security incident that may
16 potentially occur; and
17 (b) the incident is not a major cyber security incident or the
18 potential incident would not be a major cyber security
19 incident;
20 the National Cyber Security Coordinator may only make a record
21 of, use or disclose the information for the purposes of:
22 (c) directing the impacted entity to other services that may assist
23 the entity to respond to, mitigate, or resolve the incident; or
24 (d) coordinating the whole of Government response to the cyber
25 security incident where the National Cyber Security
26 Coordinator considers such a response is necessary; or
27 (e) informing and advising the Minister, and other Ministers of
28 the Commonwealth, about the cyber security incident.
29 (2) Subsection (1) does not prohibit the recording, use or disclosure of
30 the following information:
31 (a) information that has been provided by, or on behalf of, the
32 entity to the Commonwealth about the cyber security incident
33 to comply with:
34 (i) a requirement in Part 3 of this Act; or

Part 4 Coordination of major cyber security incidents
Division 3 Protection of information

Section 35

- (ii) a requirement in Part 2B of the *Security of Critical Infrastructure Act 2018*; or
- (iii) a requirement under the *Telecommunications Act 1997*; or
- (iv) a requirement under a law prescribed by the rules;
- (b) information that has been provided voluntarily to the National Cyber Security Coordinator by, or on behalf of, the entity, other than under this Part;
- (c) information that has already been lawfully made available to the public.

35 Limitations on secondary use and disclosure

- (1) An entity or a Commonwealth body (other than ASD) who obtains information under subsection 33(1), subsection 34(1) or this section, may only make a record of, use or disclose the information for a purpose that is any of the following:
 - (a) a permitted cyber security purpose;
 - (b) for an intelligence agency—the purposes of its functions;
 - (c) for a Commonwealth enforcement body—the purposes of its functions relating to the investigation or enforcement of a criminal offence.
- Note: For ASD, see Division 1A of Part 6 of the *Intelligence Services Act 2001*.
- (2) Subsection (1) does not prohibit the recording, use or disclosure of the following information:
 - (a) information referred to in subsection 33(2) or 34(2);
 - (b) if the entity is an individual—personal information about the individual;
 - (c) if the entity is the impacted entity that originally gave the information to the National Cyber Security Coordinator under section 31 or as referred to in subsection 34(1)—the impacted entity’s own information.
- (3) An entity is liable to a civil penalty if:
 - (a) the entity contravenes subsection (1); and

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- (b) the entity is not:
- (i) a Commonwealth officer; or
- (ii) an officer or employee of a State body; and
- (c) any of the following applies:
- (i) the information is sensitive information about a person and the person has not consented to the record, use or disclosure of the information;
- (ii) the information is confidential or commercially sensitive;
- (iii) the record, use or disclosure of the information would, or could reasonably be expected to, cause damage to the security, defence or international relations of the Commonwealth.
- Note 1: See the *Criminal Code* for offences for Commonwealth officers.
- Note 2: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.
- Civil penalty: 50 penalty units.

- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 36 Admissibility of information voluntarily given by impacted entity**
- (1) Information given by an entity (the **impacted entity**), or on behalf of the impacted entity, to the National Cyber Security Coordinator under section 31 or as referred to in section 34 is not admissible in evidence against the impacted entity in:
- (a) criminal proceedings for an offence against a Commonwealth law, other than:
- (i) proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* (which deal with false or misleading information or documents) that relates to this Act; or
- (ii) proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act; or

Part 4 Coordination of major cyber security incidents**Division 3** Protection of information**Section 37**

- 1 (b) civil proceedings for a contravention of a civil penalty
2 provision of a Commonwealth law, other than a civil penalty
3 provision of this Part.
- 4 (2) This section does not limit or affect any right, privilege or
5 immunity that the entity has, apart from this section, as a defendant
6 in any proceedings.

37 National Cyber Security Coordinator not compellable as witness

- 8 (1) The Secretary may issue a certificate stating that a specified person
9 who is, or has been:
- 10 (a) a person referred to in paragraph (a) of the definition of
11 **National Cyber Security Coordinator** in section 9; or
12 (b) a person referred to in paragraph (b) of the definition of
13 **National Cyber Security Coordinator** in section 9;
14 is involved, or has been involved, in the performance of the
15 National Cyber Security Coordinator's functions or exercise of the
16 National Cyber Security Coordinator's powers under this Part in
17 relation to a specified matter.
- 18 (2) If, under subsection (1), the Secretary issues a certificate in relation
19 to a person and a specified matter, the person:
- 20 (a) is not obliged to comply with a subpoena or similar direction
21 of a federal court to attend and answer questions relating to
22 the matter; and
23 (b) is not compellable to give an expert opinion in any civil or
24 criminal proceedings in a federal court in relation to the
25 matter.
- 26 (3) This section does not apply to a coronial inquiry.

Division 4—Miscellaneous

38 Interaction with other requirements to provide information in relation to a cyber security incident

Information provided by an entity under this Part does not affect any other requirement of the entity to provide that information under this Act or another law of the Commonwealth.

Note: For example, the entity may also be required to provide some or all of the information under Part 3 of this Act, Part 2B of the *Security of Critical Infrastructure Act 2018* or under the *Telecommunications Act 1997*.

Part 5 Cyber Incident Review Board
Division 1 Preliminary

Section 39

Part 5—Cyber Incident Review Board

Division 1—Preliminary

39 Simplified outline of this Part

The Cyber Incident Review Board is established by this Part.

The Board undertakes reviews of certain cyber security incidents and makes recommendations to government and industry about actions that could be taken to prevent, detect, respond to or minimise the impact of, incidents of a similar nature in the future.

Division 2—Reviews by the Board

40 Reviews by the Board

- (1) The Cyber Incident Review Board may cause a review to be conducted under this section in relation to a cyber security incident, or a series of related cyber security incidents, on written referral by:
- (a) the Minister; or
 - (b) the National Cyber Security Coordinator; or
 - (c) an entity impacted by the incident or an incident in the series of incidents; or
 - (d) a member of the Board.
- (2) A review may only be conducted under this section:
- (a) if the Board is satisfied that the incident or series of incidents meets the criteria mentioned in subsection (3); and
 - (b) after the incident or series of incidents, and the immediate response, has ended; and
 - (c) if the Minister has approved the terms of reference for the review.
- Note: The Board may, in accordance with the terms of reference for a review, appoint members of the Expert Panel to assist the Board in conducting a review: see section 61.
- (3) For the purposes of paragraph (2)(a), the criteria are:
- (a) the incident or series of incidents have seriously prejudiced, or are likely to seriously prejudice:
 - (i) the social or economic stability of Australia or its people; or
 - (ii) the defence of Australia; or
 - (iii) national security; or
 - (b) the incident or series of incidents involved novel or complex methods or technologies, an understanding of which will significantly improve Australia’s preparedness, resilience, or response to cyber security incidents of a similar nature; or

Part 5 Cyber Incident Review Board
Division 2 Reviews by the Board

Section 41

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- (c) the incident or series of incidents are, or are likely to be, of serious concern to the Australian people.
- (4) The rules may make provision for or in relation to reviews by the Board under this Part, including for or in relation to the following:
- (a) terms of reference for reviews;
- (b) notification of reviews;
- (c) the timing of when reviews may be conducted;
- (d) when reviews may be discontinued;
- (e) how information or submissions may be provided to the Board.

41 Board may discontinue a review

- 11
- 12
- 13
- 14
- 15
- (1) The Board may discontinue a review at any time.
- (2) The Board must, within 28 days of discontinuing a review, make publicly available, in any way the Board considers appropriate, a statement setting out the reasons for discontinuing the review.

42 Board may request information or documents

- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- If the Board reasonably believes that:
- (a) an entity; or
- (b) a Commonwealth body or a State body; or
- (c) an officer or employee of a Commonwealth body or a State body;
- has information or documents relevant to a review, the Chair may request, by notice in writing, the entity, body, officer or employee to give the Board such information or documents as are specified in the request.
- Note 1: There is no requirement to comply with the request.
- Note 2: The Chair may require certain entities to give documents under section 43.

43 Board may require certain entities to produce documents

- (1) This section applies if:
- (a) the Board reasonably believes that an entity involved in a cyber security incident that relates to a review has a document that is relevant to the review; and
 - (b) the Chair of the Board has requested that the entity provide the document under section 42; and
 - (c) the entity is not:
 - (i) a Commonwealth body or a State body (other than a body that is a responsible entity for a critical infrastructure asset to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies); or
 - (ii) an officer or employee of a Commonwealth body or a State body (other than a body that is a responsible entity for a critical infrastructure asset to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies).
- (2) The Chair of the Board may, by notice in writing given to the entity, require the entity to:
- (a) produce any such documents; or
 - (b) make copies of any such documents and to produce those copies;
- to the Board within the period (which must not be less than 14 days), and in the manner, specified in the notice.
- (3) The notice must set out the effect of the following provisions:
- (a) section 44;
 - (b) Part 6 of this Act (Regulatory powers);
 - (c) sections 137.1 and 137.2 of the *Criminal Code* (false or misleading information or documents).

Compensation

- (4) An entity is entitled to be paid by the Commonwealth reasonable compensation for complying with a requirement covered by paragraph (2)(b).

Part 5 Cyber Incident Review Board
Division 2 Reviews by the Board

Section 44

44 Civil penalty—failing to comply with a notice to produce documents

- (1) An entity is liable to a civil penalty if:
- (a) the entity is given a notice under subsection 43(2); and
 - (b) the entity fails to comply with the notice.

Civil penalty: 50 penalty units.

- (2) Subsection (1) does not apply in relation to the production of a document or a copy of a document if the production would, or could reasonably be expected to, prejudice one or more of the following:
- (a) the security, defence or international relations of the Commonwealth;
 - (b) the capabilities of an intelligence agency;
 - (c) the prevention, detection or investigation of, or the conduct of proceedings relating to, an offence or a contravention of a civil penalty provision;
 - (d) the administration of justice.
- (3) Subsection 93(2) of the Regulatory Powers Act does not apply in relation to a contravention of subsection (1) of this section.
- (4) Despite section 96 of the Regulatory Powers Act, in proceedings for a civil penalty order against an entity for a contravention of subsection (1), the entity does not bear an evidential burden in relation to the matters in subsection (2).

Note: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.

45 Draft review reports

- (1) If:
- (a) the Board proposes to include information in a final review report prepared under section 46; and
 - (b) the Board considers that the information may be sensitive review information;

Section 46

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- then the Board may consult an entity, a Commonwealth body or a State body that has an interest in the information about whether the information is sensitive review information.
- Note: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 47.
- (2) The Board may consult the entity or body in any way the Board considers appropriate, including by providing a draft report, or an extract of a draft report (a **draft review report**).
- Note: Section 52 prohibits making a record of, disclosing or using information contained in a draft review report, except in limited circumstances.
- (3) The Board must specify a reasonable period within which the entity or body may make any submissions to the Board.
- (4) Submissions must be given in the manner and form (if any) prescribed by the rules.
- (5) However, this section does not authorise the Board to use or disclose information the use or disclosure of which is prohibited or restricted by or under this Act, another Act or an instrument made under an Act.

20 **46 Final review reports**

- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- (1) After completing a review under section 40, the Board must prepare a report (a **final review report**) on the review.
- Note 1: The Board must redact sensitive review information from a final review report: see section 47.
- Note 2: If information is redacted from a final review report, the Board must also prepare a protected review report: see section 48.
- (2) In preparing the final review report, the Board must consider any submissions received in response to any consultation undertaken under section 45 about whether information is sensitive review information.
- (3) Subject to section 47, the final review report must set out:
- (a) any recommendations that the Board thinks fit to make; and

Part 5 Cyber Incident Review Board
Division 2 Reviews by the Board

Section 47

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- (b) if recommendations are made—the reasons for those recommendations; and
- (c) if the terms of reference for the review require particular information to be included in the review report—that information; and
- (d) information (if any) that is prescribed by the rules; and
- (e) such other information that the Board thinks fit to include in the report.
- (4) The final review report must not:
- (a) apportion blame in relation to a cyber security incident that was the subject of the review; or
- (b) provide the means to determine the liability of any entity in relation to such a cyber security incident; or
- (c) identify an individual (unless the individual has consented).
- This section does not otherwise limit what may be included in a review report.
- (5) The Board must publish the final review report (excluding any information required to be redacted under section 47). The report may be published in any way the Board considers appropriate.

47 Certain information must be redacted from final review reports

- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- (1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.
- Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 48.
- (2) **Sensitive review information** is information the disclosure of which:
- (a) could prejudice the security, defence or international relations of Australia; or
- (b) would prejudice relations between the Commonwealth government and the government of a State or Territory; or

Section 48

- (c) could reveal, or enable a person to ascertain, the existence or identity of a confidential source of information in relation to the enforcement of the criminal law; or
- (d) could reveal, or enable a person to ascertain, the identity of a person who is, or has been, a staff member of an intelligence agency; or
- (e) could endanger a person’s life or physical safety; or
- (f) would prejudice the fair trial of any person or the impartial adjudication of a matter; or
- (g) would involve disclosing information whose disclosure is prohibited or restricted by or under this Act, another Act or an instrument made under an Act; or
- (h) would involve unreasonably disclosing confidential commercial information; or
- (i) would involve the disclosure of personal information about an individual without their consent.

48 Protected review reports

- (1) If information must be redacted from a final review report under section 47, the Board must prepare another report (a **protected review report**) that includes:
 - (a) the redacted information; and
 - (b) the reasons for redacting the information from the final review report.
- (2) If a protected review report is prepared under this section, the Board must give the Minister, and the Prime Minister, a copy of:
 - (a) the final review report prepared under section 46; and
 - (b) a copy of the protected review report.
- (3) The Board may give a copy of a protected review report, or an extract of a protected review report, to:
 - (a) a Commonwealth body; or
 - (b) a State body; or
 - (c) an entity;for a permitted cyber security purpose.

Part 5 Cyber Incident Review Board
Division 2 Reviews by the Board

Section 48

- 1
- 2
- 3
- (4) However, this section does not authorise the Board to use or disclose information the use or disclosure of which is prohibited or restricted by or under this Act or another Commonwealth law.

Division 3—Protection of information relating to reviews

**Subdivision A—Protection of information requested or
required by the Board**

49 Limitations on use and disclosure by the Board

The Board may only make a record of, use or disclose information provided by an entity, Commonwealth body or State body under section 42 or 43 if making the record of, using or disclosing the information is:

- (a) for a purpose that is any of the following:
 - (i) the purposes of performing functions or exercising powers under this Part or Part 6 as it applies to this Part;
 - (ii) the purposes of proceedings under, or arising out of, section 137.1 or 137.2 of the *Criminal Code* (false and misleading information and documents) that relate to this Act;
 - (iii) the purposes of proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act;
 - (iv) a permitted cyber security purpose; or
- (b) otherwise authorised by a provision of this Part.

Note 1: For permitted cyber security purposes: see subsection 33(3).

Note 2: See the *Criminal Code* for offences for Commonwealth officers.

50 Limitations on secondary use and disclosure

- (1) An entity or a Commonwealth body who obtains information under section 49, or this section, may only make a record of, use or disclose the information:
 - (a) for a purpose that is any of the following:
 - (i) the purposes of performing functions or exercising powers under this Part or Part 6 as it applies to this Part;

Part 5 Cyber Incident Review Board

Division 3 Protection of information relating to reviews

Section 50

- 1 (ii) the purposes of proceedings under, or arising out of,
2 section 137.1 or 137.2 of the *Criminal Code* (false and
3 misleading information and documents) that relate to
4 this Act;
- 5 (iii) the purposes of proceedings for an offence against
6 section 149.1 of the *Criminal Code* (which deals with
7 obstruction of Commonwealth public officials) that
8 relates to this Act;
- 9 (iv) a permitted cyber security purpose;
- 10 (v) for an intelligence agency—for the purposes of its
11 functions;
- 12 (vi) for a Commonwealth enforcement body—for purposes
13 of its functions relating to the investigation or
14 enforcement of a criminal offence; or
- 15 (b) if otherwise authorised by a provision of this Part.
- 16 (2) Subsection (1) does not prohibit the recording, use or disclosure of
17 the following information:
 - 18 (a) information that has already been lawfully made available to
19 the public (for example, in the publication of the final review
20 report);
 - 21 (b) if the entity is an individual—personal information about the
22 individual;
 - 23 (c) if the entity or body is the entity or body that originally
24 provided the information under section 42 or 43—the entity’s
25 or body’s own information.
- 26 (3) An entity is liable to a civil penalty if:
 - 27 (a) the entity contravenes subsection (1); and
 - 28 (b) the entity is not:
 - 29 (i) a Commonwealth officer; or
 - 30 (ii) an officer or employee of a State body; and
 - 31 (c) any of the following applies:
 - 32 (i) the information is sensitive information about a person
33 and the person has not consented to the record, use or
34 disclosure of the information;

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- (ii) the information is confidential or commercially sensitive;
- (iii) the record, use or disclosure of the information would, or could reasonably be expected to, cause damage to the security, defence or international relations of the Commonwealth.
- Note 1: See the *Criminal Code* for offences for Commonwealth officers.
- Note 2: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.
- Civil penalty: 50 penalty units.

51 Admissibility of information voluntarily given to the Board

- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- (1) Information given by an entity to the Board under section 42 is not admissible in evidence against the entity in:
- (a) criminal proceedings for an offence under a Commonwealth law, other than:
- (i) proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* (which deal with false or misleading information or documents) that relates to this Act; or
- (ii) proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act; or
- (b) civil proceedings for a contravention of a civil penalty provision of a Commonwealth law, other than a civil penalty provision of this Part.
- (2) This section does not limit or affect any right, privilege or immunity that the entity has, apart from this section, as a defendant in any proceedings.

Part 5 Cyber Incident Review Board
Division 3 Protection of information relating to reviews

Section 52

Subdivision B—Protection of reports

52 Disclosure of draft review reports prohibited

- (1) An entity is liable to a civil penalty if:
- (a) the entity receives a draft review report under section 45; and
 - (b) the entity makes a record of, discloses or otherwise uses any information in the draft review report.

Civil penalty: 50 penalty units.

- (2) Subsection (1) does not apply if the making of the record, disclosure or use is:
- (a) for the purpose of preparing a submission to the Board in accordance with section 45; or
 - (b) with the consent of the Chair of the Board; or
 - (c) after the information has already been lawfully made available to the public (for example, in the publication of the final review report).

- (3) Despite section 96 of the Regulatory Powers Act, in proceedings for a civil penalty order against an entity for a contravention of subsection (1), the entity does not bear an evidential burden in relation to the matters in subsection (2).

Note: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.

53 Disclosure of protected review reports prohibited

- (1) An entity is liable to a civil penalty if:
- (a) the entity is given a copy of a protected review report under section 48; and
 - (b) the entity makes a record of, discloses or otherwise uses information contained in the protected review report.

Civil penalty: 50 penalty units.

- (2) Subsection (1) does not apply if the making of the record, disclosure or use is:

Section 53

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- (a) authorised by section 48; or
- (b) after the information has already been lawfully made
available to the public (for example, in the publication of the
final review report).
- Civil penalty: 50 penalty units.
- (3) Despite section 96 of the Regulatory Powers Act, in proceedings
for a civil penalty order against an entity for a contravention of
subsection (1), the entity does not bear an evidential burden in
relation to the matters in subsection (2).
- Note: This Act does not make the Crown (other than an authority of the
Crown) liable to a civil penalty.

Part 5 Cyber Incident Review Board
Division 4 Establishment, functions and powers of the Board

Section 54

Division 4—Establishment, functions and powers of the Board

54 Cyber Incident Review Board

- (1) The Cyber Incident Review Board is established by this section.
 - (2) For the purposes of paragraph (a) of the definition of **Department of State** in section 8 of the *Public Governance, Performance and Accountability Act 2013*, the Cyber Incident Review Board is prescribed in relation to the Department.
- Note: Subject to subsection (2), this means that the Board members are officials of the Department for the purposes of the *Public Governance, Performance and Accountability Act 2013*.

55 Constitution of the Board

- The Board consists of the following members:
- (a) a Chair;
 - (b) at least 2, and not more than 6, other members.

56 Functions of the Board

- (1) The functions of the Board are:
 - (a) to review cyber security incidents, or series of related cyber security incidents, to:
 - (i) identify factors that contributed to the incident or series of incidents; and
 - (ii) make recommendations to government and industry about actions that could be taken to prevent, detect, respond to or minimise the impact of, incidents of a similar nature in the future; and
 - (iii) report publicly on the review; and
 - (b) any other functions conferred on the Board by this Act or the rules.
- Note: See section 40 in relation to the circumstances in which a cyber security incident may be reviewed by the Board.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- (2) It is not a function of the Board to:
- (a) apportion blame in relation to a cyber security incident; or
- (b) to provide the means to determine the liability of any entity in relation to a cyber security incident.
- (3) The Board has power to do all things necessary or convenient to be done for or in connection with the performance of the Board’s functions.
- (4) The rules may prescribe the circumstances in which cyber security incidents are a series of related incidents for the purposes of this section.
- Note: For example, the rules may prescribe that cyber security incidents are a series of related incidents if the incidents involve a common type of impacted system or a common attack method.

14 **57 Independence**

- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- Subject to this Act and to other laws of the Commonwealth, the Cyber Incident Review Board:
- (a) has complete discretion in the performance of the Board’s functions and the exercise of the Board’s powers; and
- (b) is not subject to direction by any person in relation to the performance or exercise of those functions or powers.
- Note: The Minister must approve the terms of reference for a review to be undertaken by the Board: see subsection 40(2).

Part 5 Cyber Incident Review Board
Division 5 Terms and conditions of appointment of Board members

Section 58

Division 5—Terms and conditions of appointment of Board members

58 Appointment of Board members

- (1) A Board member is to be appointed by the Minister by written instrument.
Note: A Board member may be reappointed: see section 33AA of the *Acts Interpretation Act 1901*.
- (2) A Board member may be appointed on a full-time or part-time basis.
- (3) A Board member holds office for the period specified in the instrument of appointment. The period must not exceed 4 years.
- (4) The rules may make provision for or in relation to the appointment of Board members, including in relation to eligibility for appointment.

59 Acting Chair

- The Minister may, by written instrument, appoint a Board member to act as the Chair:
- (a) during a vacancy in the office of Chair (whether or not an appointment has previously been made to the office); or
 - (b) during any period, or during all periods, when the Chair:
 - (i) is absent from duty or from Australia; or
 - (ii) is, for any reason, unable to perform the duties of the office.
- Note: For rules that apply to acting appointments, see section 33A of the *Acts Interpretation Act 1901*.

60 Terms and conditions etc. for members

- (1) The rules may make provision for or in relation to the Board, including for or in relation to the following:
 - (a) membership of the Board (subject to section 55);

Section 60

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- (b) terms of appointment of members;
- (c) acting appointments;
- (d) remuneration of members;
- (e) resignation of members;
- (f) disclosure of interests by members;
- (g) termination of appointment of members;
- (h) leave of absence of members.
- (2) A member of the Board holds office on the terms and conditions (if any) that are determined by the Minister in relation to matters not covered by this Act or the rules.

Part 5 Cyber Incident Review Board
Division 6 Expert Panel, staff assisting and consultants

Section 61

Division 6—Expert Panel, staff assisting and consultants

61 Expert Panel

- (1) The Board may, in writing, establish an Expert Panel.
- (2) The Expert Panel consists of such members as the Board from time to time appoints by written instrument.

Note: A member of the Expert Panel may be reappointed: see section 33AA of the *Acts Interpretation Act 1901*.
- (3) One or more members of the Expert Panel are to be appointed, in writing and in accordance with the terms of reference for a review under section 40, to assist the Board in the performance of its functions or the exercise of its powers in relation to the review.
- (4) An appointment to the Expert Panel, or an appointment to assist in a review, is not a public office within the meaning of the *Remuneration Tribunal Act 1973*.
- (5) The rules may make provision for or in relation to the Expert Panel, including for or in relation to the following:
 - (a) membership of the Expert Panel;
 - (b) appointment of members to the Expert Panel;
 - (c) appointments of its members to assist the Board in relation to a review;
 - (d) terms of appointment of members;
 - (e) remuneration of members;
 - (f) resignation of members;
 - (g) disclosure of interests by members;
 - (h) termination of appointment of members;
 - (i) leave of absence of members.

62 Arrangements relating to staff of the Department

- (1) The staff assisting the Cyber Incident Review Board are to be APS employees, or officers or employees of a Commonwealth body, whose services are made available to the Board in connection with

Section 63

- 1
- 2
- 3
- 4
- the performance of any of the Board’s functions or the exercise of any of the Board’s powers.
- (2) When performing services for the Board, the staff are subject to the directions of the Board.

5

63 Consultants

6

7

8

9

The Secretary of the Department may, on behalf of the Commonwealth, engage consultants to assist in the performance of any of the Cyber Incident Review Board’s functions or the exercise of any of the Board’s powers.

Part 5 Cyber Incident Review Board**Division 7** Other matters relating to the BoardSection 64

1 **Division 7—Other matters relating to the Board**2 **64 Board procedures**

- 3 (1) Subject to this Act and the rules, the Board may:
- 4 (a) operate in the way it determines; and
- 5 (b) regulate proceedings at its meetings as it considers
- 6 appropriate.
- 7 (2) The rules may make provision for or in relation to the operation
- 8 and procedures of the Board.

9 **65 Liability**10 *Responding to notices to produce*

- 11 (1) An entity is not liable to an action or other proceeding for damages
- 12 for or in relation to an act done or omitted in good faith in
- 13 compliance with section 43 (Chair may obtain documents from
- 14 certain entities).
- 15 (2) An officer, employee or agent of an entity is not liable to an action
- 16 for damages for or in relation to an act done or omitted in good
- 17 faith in connection with an act done or omitted by the entity as
- 18 mentioned in subsection (1).

19 *The Board etc.*

- 20 (3) A person who is or has been:
- 21 (a) a Board member; or
- 22 (b) a member of the Expert Panel; or
- 23 (c) a member of the staff assisting the Board (as mentioned in
- 24 section 62); or
- 25 (d) a consultant assisting the Board (as mentioned in section 63);
- 26 is not liable to an action or other proceeding for damages for or in
- 27 relation to an act done or omitted in good faith in the performance
- 28 or purported performance of a function or duty conferred by this

Section 66

1 Part, or the exercise or purported exercise of a power conferred by
2 this Part.

3 *Evidential burden*

4 (4) An entity or person who wishes to rely on subsection (1), (2) or (3)
5 in relation to an action or other proceeding bears an evidential
6 burden (within the meaning of the Regulatory Powers Act) in
7 relation to that matter.

8 **66 Certification of involvement in review**

9 (1) The Chair of the Board may issue a certificate stating that a
10 specified person who is, or has been:
11 (a) a Board member; or
12 (b) a member of the Expert Panel; or
13 (c) a member of the staff assisting the Board (as mentioned in
14 section 62); or
15 (d) a consultant assisting the Board (as mentioned in section 63);
16 is involved, or has been involved, in a review under this Part into a
17 specified matter.

18 (2) If, under subsection (1), the Board issues a certificate in relation to
19 a person and a specified matter, the person:
20 (a) is not obliged to comply with a subpoena or similar direction
21 of a federal court to attend and answer questions relating to
22 the matter; and
23 (b) is not compellable to give an expert opinion in any civil or
24 criminal proceedings in a federal court in relation to the
25 matter.

26 (3) This section does not apply to a coronial inquiry.

27 **67 Annual report**

28 The annual report prepared by the Secretary and given to the
29 Minister under section 46 of the *Public Governance, Performance*

Section 67

1 **Part 6—Regulatory powers**

2 **Division 1—Preliminary**

3 **68 Simplified outline of this Part**

4 Each civil penalty provision of this Act, and Division 1A of Part 6
5 of the *Intelligence Services Act 2001*, is subject to:
6 (a) monitoring under Part 2 of the Regulatory Powers Act;
7 and
8 (b) investigation under Part 3 of the Regulatory Powers Act.

9 Civil penalty orders may be sought under Part 4 of the Regulatory
10 Powers Act from a relevant court in relation to contraventions of
11 such civil penalty provisions.

12 Infringement notices may be given under Part 5 of the Regulatory
13 Powers Act for alleged contraventions of such civil penalty
14 provisions.

15 Undertakings to comply with such civil penalty provisions may be
16 accepted and enforced under Part 6 of the Regulatory Powers Act.

17 Injunctions under Part 7 of the Regulatory Powers Act may be used
18 to restrain a person from contravening, or to compel compliance
19 with, a civil penalty provision.

Part 6 Regulatory powers
Division 2 Civil penalty provisions, enforceable undertakings and injunctions

Section 69

Division 2—Civil penalty provisions, enforceable undertakings and injunctions

69 Civil penalty provisions, enforceable undertakings and injunctions

Enforceable civil penalty provisions

- (1) Each civil penalty provision of this Act, and each civil penalty of Division 1A of Part 6 of the *Intelligence Services Act 2001*, is enforceable under:
- (a) Part 4 of the Regulatory Powers Act (civil penalty provisions); and
 - (b) Part 6 of that Act (enforceable undertakings); and
 - (c) Part 7 of that Act (injunctions).

- Note 1: Part 4 of the Regulatory Powers Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.
- Note 2: Part 6 of that Act creates a framework for accepting and enforcing undertakings relating to compliance with provisions.
- Note 3: Part 7 of that Act creates a framework for using injunctions to enforce provisions.

Authorised applicant

- (2) For the purposes of Part 4 of the Regulatory Powers Act, each of the following persons is an authorised applicant in relation to the civil penalty provisions mentioned in subsection (1):
- (a) the Secretary;
 - (b) a person who is appointed under subsection (3).
- (3) For the purposes of paragraph (2)(b), the Secretary may, by writing, appoint a person who:
- (a) is the chief executive officer (however described) of a designated Commonwealth body; or
 - (b) is an SES employee, or an acting SES employee, in:
 - (i) the Department; or

- 1
- (ii) a designated Commonwealth body; or
- 2
- (c) holds, or is acting in, a position in a designated
- 3
- Commonwealth body that is equivalent to, or higher than, a
- 4
- position occupied by an SES employee;
- 5
- to be an authorised applicant for the purposes of Part 4 of the
- 6
- Regulatory Powers Act.

7

Note:

8

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

9

Authorised person

- 10
- (4) For the purposes of Parts 6 and 7 of the Regulatory Powers Act, as
- 11
- those Parts apply in relation to a civil penalty provision mentioned
- 12
- in subsection (1), each of the following persons is an authorised
- 13
- person:
- 14
- (a) the Secretary;
- 15
- (b) a person who is appointed under subsection (5).
- 16
- (5) For the purposes of paragraph (2)(b), the Secretary may, by
- 17
- writing, appoint a person who is an SES employee, or an acting
- 18
- SES employee in:
- 19
- (a) the Department; or
- 20
- (b) a designated Commonwealth body.

21

Note:

22

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

23

Relevant court

- 24
- (6) For the purposes of Part 4 of the Regulatory Powers Act, each of
- 25
- the following courts is a relevant court in relation to the civil
- 26
- penalty provisions mentioned in subsection (1):
- 27
- (a) the Federal Court of Australia;
- 28
- (b) the Federal Circuit and Family Court of Australia
- 29
- (Division 2);
- 30
- (c) a court of a State or Territory that has jurisdiction in relation
- 31
- to the matter.

Part 6 Regulatory powers
Division 2 Civil penalty provisions, enforceable undertakings and injunctions

Section 69

- 1
- 2
- 3
- 4
- 5
- 6
- Liability of Crown*

(7) Part 4 of the Regulatory Powers Act, as that Part applies in relation to the civil penalty provisions mentioned in subsection (1), does not make the Crown liable to a pecuniary penalty.

(8) The protection in subsection (7) does not apply to an authority of the Crown.

Division 3—Monitoring and investigation powers

70 Monitoring powers

Provisions subject to monitoring

- (1) A provision is subject to monitoring under Part 2 of the Regulatory Powers Act if it is a civil penalty provision of this Act or of Division 1A of Part 6 of the *Intelligence Services Act 2001*.

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether the provisions have been complied with. It includes powers of entry and inspection.

Information subject to monitoring

- (2) Information given in compliance or purported compliance with a civil penalty provision mentioned in subsection (1) is subject to monitoring under Part 2 of the Regulatory Powers Act.

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether the information is correct. It includes powers of entry and inspection.

Authorised applicant

- (3) For the purposes of Part 2 of the Regulatory Powers Act, a person who is appointed under subsection (4) is an authorised applicant in relation to the civil penalty provisions mentioned in subsection (1) and information mentioned in subsection (2).
- (4) The Secretary may, by writing, appoint a person who:
- (a) is an SES employee, or an acting SES employee, in:
 - (i) the Department; or
 - (ii) a designated Commonwealth body; or
 - (b) holds, or is acting in, a position in a designated Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee;
- to be an authorised applicant in relation to the civil penalty provisions mentioned in subsection (1) and information mentioned in subsection (2).

Part 6 Regulatory powers
Division 3 Monitoring and investigation powers

Section 70

- 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
- Note: The expressions **SES employee** and **acting SES employee** are defined in section 2B of the *Acts Interpretation Act 1901*.
- Authorised person*
- (5) For the purposes of Part 2 of the Regulatory Powers Act, a person who is appointed under subsection (6) is an authorised person in relation to the civil penalty provisions mentioned in subsection (1) and information mentioned in subsection (2).
- (6) The Secretary may, by writing, appoint a person who is:
- (a) an APS employee in:

(i) the Department; or

(ii) a designated Commonwealth body; or

(b) an officer or employee of a designated Commonwealth body;
- to be an authorised person in relation to the civil penalty provisions mentioned in subsection (1) and information mentioned in subsection (2).
- Issuing officer*
- (7) For the purposes of Part 2 of the Regulatory Powers Act, a magistrate is an issuing officer in relation to the civil penalty provisions mentioned in subsection (1) and information mentioned in subsection (2).
- Relevant chief executive*
- (8) For the purposes of Part 2 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to the civil penalty provisions mentioned in subsection (1) and information mentioned in subsection (2).
- Relevant court*
- (9) For the purposes of Part 2 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the civil penalty provisions mentioned in subsection (1) and information mentioned in subsection (2):
- (a) the Federal Court of Australia;

- (b) the Federal Circuit and Family Court of Australia (Division 2);
- (c) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

Premises

- (10) An authorised person must not enter premises under Part 2 of the Regulatory Powers Act, as it applies in relation to the civil penalty provisions mentioned in subsection (1) and information mentioned in subsection (2), if the premises are used solely or primarily as a residence.

71 Investigation powers

Provisions subject to investigation

- (1) A provision is subject to investigation under Part 3 of the Regulatory Powers Act if it is a civil penalty provision of this Act or of Division 1A of Part 6 of the *Intelligence Services Act 2001*.

Authorised applicant

- (2) For the purposes of Part 3 of the Regulatory Powers Act, a person who is appointed under subsection (3) is an authorised applicant in relation to evidential material that relates to a civil penalty provision mentioned in subsection (1).
- (3) The Secretary may, by writing, appoint a person who:
 - (a) is an SES employee, or an acting SES employee, in:
 - (i) the Department; or
 - (ii) a designated Commonwealth body; or
 - (b) holds, or is acting in, a position in a designated Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee;to be an authorised applicant in relation to evidential material that relates to a civil penalty provision mentioned in subsection (1).

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

Section 71

Division 4—Infringement notices

72 Infringement notices

Provisions subject to an infringement notice

- (1) A civil penalty provision of this Act or of Division 1A of Part 6 of the *Intelligence Services Act 2001* is subject to an infringement notice under Part 5 of the Regulatory Powers Act.

Note: Part 5 of the Regulatory Powers Act creates a framework for using infringement notices in relation to provisions.

Infringement officer

- (2) For the purposes of Part 5 of the Regulatory Powers Act, a person authorised under subsection (3) is an infringement officer in relation to the civil penalty provisions mentioned in subsection (1).
- (3) The Secretary may, by writing, authorise a person who:
- (a) is an SES employee, or an acting SES employee, in:
 - (i) the Department; or
 - (ii) a designated Commonwealth body; or
 - (b) holds, or is acting in, a position in a designated Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee;
- to be an infringement officer in relation to the civil penalty provisions mentioned in subsection (1).

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

Relevant chief executive

- (4) For the purposes of Part 5 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to the civil penalty provisions mentioned in subsection (1).
- (5) The relevant chief executive may, in writing, delegate any or all of the relevant chief executive’s powers and functions under Part 5 of

Part 6 Regulatory powers
Division 4 Infringement notices

Section 72

- 1 the Regulatory Powers Act to a person who is an SES employee or
2 an acting SES employee in:
3 (a) the Department; or
4 (b) a designated Commonwealth body.

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

- 7 (6) A person exercising powers or performing functions under a
8 delegation under subsection (5) must comply with any directions of
9 the relevant chief executive.

10 *Liability of Crown*

- 11 (7) Part 5 of the Regulatory Powers Act, as that Part applies in relation
12 to the civil penalty provisions mentioned in subsection (1), does
13 not make the Crown liable to be given an infringement notice.
14 (8) The protection in subsection (7) does not apply to an authority of
15 the Crown.

1 **Division 5—Other matters**

2 **73 Contravening a civil penalty provision**

- 3 (1) This section applies if a provision of this Act provides that an
4 entity contravening another provision of this Act (the **conduct**
5 **provision**) is liable to a civil penalty.
- 6 (2) For the purposes of this Act, and the Regulatory Powers Act to the
7 extent that it relates to this Act, a reference to a contravention of a
8 civil penalty provision includes a reference to a contravention of
9 the conduct provision.

Part 7 Miscellaneous

Section 74

Part 7—Miscellaneous

74 Simplified outline of this Part

This Part deals with miscellaneous matters, such as delegations and rules.

75 How this Act applies in relation to non-legal persons

How permissions and rights are conferred and exercised

- (1) If this Act purports to confer a permission or right on an entity that is not a legal person, the permission or right:
 - (a) is conferred on each person who is an accountable person for the entity at the time the permission or right may be exercised; and
 - (b) may be exercised by:
 - (i) any person who is an accountable person for the entity at the time the permission or right may be exercised; or
 - (ii) any person who is authorised by a person referred to in subparagraph (i) to exercise the permission or right.

How obligations and duties are imposed and discharged

- (2) If this Act purports to impose an obligation or duty on an entity that is not a legal person, the obligation or duty:
 - (a) is imposed on each person who is an accountable person for the entity at the time the obligation or duty arises or is in operation; and
 - (b) may be discharged by:
 - (i) any person who is an accountable person for the entity at the time the obligation or duty arises or is in operation; or
 - (ii) any person who is authorised by a person referred to in subparagraph (i) to discharge the obligation or duty.

How non-legal persons contravene this Act

- (3) A provision of this Act (including a civil penalty provision) that is purportedly contravened by an entity that is not a legal person is instead contravened by each accountable person for the entity who:
- (a) did the relevant act or made the relevant omission; or
 - (b) aided, abetted, counselled or procured the relevant act or omission; or
 - (c) was in any way knowingly concerned in, or party to, the relevant act or omission.

Meaning of accountable person

- (4) For the purposes of this section, a person is an **accountable person** for an entity at a particular time if:
- (a) in the case of a partnership in which one or more of the partners is an individual—the individual is a partner in the partnership at that time; or
 - (b) in the case of a partnership in which one or more of the partners is a body corporate—the person is a director of the body corporate at that time; or
 - (c) in the case of a trust in which the trustee, or one or more of the trustees, is an individual—the individual is a trustee of the trust at that time; or
 - (d) in the case of a trust in which the trustee, or one or more of the trustees, is a body corporate—the person is a director of the body corporate at that time; or
 - (e) in the case of an unincorporated association—the person is a member of the governing body of the unincorporated association at that time.

76 Delegation by Secretary

- (1) The Secretary may, in writing, delegate all or any of the Secretary’s functions or powers under section 16, 17 or 18 to an SES employee, or acting SES employee, in the Department.
- Note: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.

Part 7 Miscellaneous

Section 77

1 (2) In performing a delegated function or exercising a delegated
2 power, the delegate must comply with any written directions of the
3 Secretary.

4 77 Rules

- 5 (1) The Minister may, by legislative instrument, make rules
6 prescribing matters:
7 (a) required or permitted by this Act to be prescribed by the
8 rules; or
9 (b) necessary or convenient to be prescribed for carrying out or
10 giving effect to this Act.
- 11 (2) To avoid doubt, the rules may not do the following:
12 (a) create an offence or civil penalty;
13 (b) provide powers of:
14 (i) arrest or detention; or
15 (ii) entry, search or seizure;
16 (c) impose a tax;
17 (d) set an amount to be appropriated from the Consolidated
18 Revenue Fund under an appropriation in this Act;
19 (e) directly amend the text of this Act.
- 20 (3) Before making or amending the rules, the Minister must:
21 (a) cause to be published on the Department’s website a notice:
22 (i) setting out the draft rules or amendments; and
23 (ii) inviting persons to make submissions to the Minister
24 about the draft rules or amendments within the period
25 specified in the notice; and
26 (b) consider any submissions received within the period
27 mentioned in subparagraph (a)(ii).
- 28 (4) The period specified in the notice must not be shorter than 28 days.
- 29

2022-2023-2024

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

EXPOSURE DRAFT

This is a limited circulation exposure draft. It is supplied in confidence and should be given appropriate protection.

**Intelligence Services and Other
Legislation Amendment (Cyber Security)
Bill 2024**

No. , 2024

(Home Affairs)

A Bill for an Act to amend the *Intelligence Services Act 2001* and make consequential amendments arising from the *Cyber Security Act 2024*, and for related purposes

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Contents

1	Short title	1
2	Commencement	2
3	Schedules	2
Schedule 1—Limited use of certain cyber security information		3
	<i>Intelligence Services Act 2001</i>	3
Schedule 2—Other amendments		12
	<i>Freedom of Information Act 1982</i>	12

1 **A Bill for an Act to amend the *Intelligence Services***
2 ***Act 2001* and make consequential amendments**
3 **arising from the *Cyber Security Act 2024*, and for**
4 **related purposes**

5 The Parliament of Australia enacts:

6 **1 Short title**

7 This Act is the *Intelligence Services and Other Legislation*
8 *Amendment (Cyber Security) Act 2024*.

No. , 2024 *Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024* 1

Released by Department of Home Affairs
under the Freedom of Information Act 1982

1
2
3
4
5
6

7
8
9

10
11
12

13

14
15
16
17

2 Commencement

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

Commencement information		
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	
2. Schedules 1 and 2	At the same time as Part 4 of the <i>Cyber Security Act 2024</i> commences.	

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

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

3 Schedules

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

Schedule 1—Limited use of certain cyber security information

Intelligence Services Act 2001

1 Subsection 3(1)

Insert:

Commonwealth body, for the purposes of Division 1A of Part 6, has the meaning given by subsection 41BB(8).

computer has the same meaning as in the *Security of Critical Infrastructure Act 2018*.

coronial inquiry means a coronial inquiry, coronial investigation or coronial inquest under a law of the Commonwealth, or of a State or Territory.

cyber security incident has the meaning given by subsection 41BA(3).

entity, for the purposes of Division 1A of Part 6, has the meaning given by subsection 41BA(5).

permitted cyber security purposes has the meaning given by subsection 41BA(4).

2 After Division 1 of Part 6

Insert:

Division 1A—Limited communication of certain cyber security information acquired by ASD

41BA Communication of certain cyber security information by ASD

- (1) The Director-General of ASD, or a staff member of ASD, may only communicate information covered by subsection (2) if the communication is for a permitted cyber security purpose.

Cyber security information covered by this subsection

(2) Information is covered by this subsection if:

(a) the information relates to:

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

(ii) a cyber security incident that may potentially occur; and

(b) the information:

(i) has been voluntarily provided to ASD in the performance of its functions, by an entity (the **impacted entity**) that is, was, or is likely to be, directly or indirectly impacted by the cyber security incident or would likely be impacted by the potential cyber security incident, or by another entity acting on behalf of the impacted entity; or

(ii) has been acquired or prepared by ASD, in the performance of its functions, with the consent of the impacted entity; or

(iii) has been acquired by the National Cyber Security Coordinator under section 25 of the *Cyber Security Act 2024* in relation to the cyber security incident and disclosed to ASD under section 27 of that Act; and

(c) the information is not any of the following:

(i) information that has been provided to the Commonwealth about the cyber security incident to comply with a requirement in Part 3 of the *Cyber Security Act 2024* or in Part 2B of the *Security of Critical Infrastructure Act 2018*, a requirement under the *Telecommunications Act 1997*, or a requirement under a prescribed law;

(ii) information that has already been lawfully made available to the public;

(iii) information that is not about an identifiable entity or a reasonably identifiable entity.

(3) A **cyber security incident** is:

(a) one or more acts, events or circumstances:

- 1 (i) of a kind covered by the meaning of **cyber security**
2 **incident** in the *Security of Critical Infrastructure Act*
3 *2018*; or
- 4 (ii) involving unauthorised impairment of electronic
5 communication to or from a computer, within the
6 meaning of that phrase in that Act, but including mere
7 interception of any such communication; or
- 8 (b) the discovery of unintended or unexpected vulnerabilities in a
9 computer, computer data or a computer program that, if
10 exploited, would result in a cyber security incident within the
11 meaning of paragraph (a).

Permitted cyber security purposes

- 12
- 13 (4) The following are **permitted cyber security purposes**:
 - 14 (a) assisting, in the performance of ASD's functions, the
15 impacted entity, and other entities acting on behalf of the
16 entity, to respond to, mitigate or resolve the cyber security
17 incident or potential cyber security incident;
 - 18 (b) providing technical advice and assistance, in the performance
19 of ASD's functions, to entities on the prevention of cyber
20 security incidents or potential cyber security incidents;
 - 21 (c) informing and advising the Minister, and other Ministers of
22 the Commonwealth, about the cyber security incident or
23 potential cyber security incident;
 - 24 (d) communicating the information to the National Cyber
25 Security Coordinator for the purposes of its functions under
26 Part 4 of the *Cyber Security Act 2024*;
 - 27 (e) communicating the information for the purposes of ASD's
28 functions;
 - 29 (f) communicating the information to:
 - 30 (i) another agency for the purposes of its functions; or
 - 31 (ii) the Australian Security Intelligence Organisation for the
32 purposes of its functions; or
 - 33 (iii) the Defence Intelligence Organisation for the purposes
34 of its functions; or
 - 35 (iv) the Office of National Intelligence for the purposes of
36 its functions; or

Schedule 1 Limited use of certain cyber security information

- (v) a Commonwealth enforcement body (within the meaning of the *Cyber Security Act 2024*) for the purposes of its functions relating to the investigation or enforcement of a criminal offence.

- (5) For the purposes of this Division, *entity* has the same meaning as in the *Cyber Security Act 2024*.

41BB Limitations on secondary use and communication

- (1) An entity or Commonwealth body who, under subsection 41BA(1) or this section, obtains information covered by subsection 41BA(2) may only make a record of, use or communicate the information for a purpose that is any of the following:
- (a) a permitted cyber security purpose;
 - (b) preventing or lessening a serious threat to the life or health of an individual or a group of individuals;
 - (c) for the National Cyber Security Coordinator—the purposes of its functions under Part 4 of the *Cyber Security Act 2024*;
 - (d) for an agency, the Australian Security Intelligence Organisation, the Defence Intelligence Organisation or the Office of National Intelligence—the purposes of its functions;
 - (e) for a Commonwealth enforcement body—the purposes of its functions relating to the investigation or enforcement of a criminal offence.
- (2) Subsection (1) does not prohibit the recording, use or communication of the following information:
- (a) if the entity is an individual—personal information (within the meaning of the *Privacy Act 1988*) about the individual;
 - (b) if the entity is the impacted entity that:
 - (i) originally provided the information to ASD as referred to in subparagraph 41BA(2)(b)(i); or
 - (ii) originally gave the information to the National Cyber Security Coordinator under section 31, or as referred to in subsection 34(1), of the *Cyber Security Act 2024*; information that is the impacted entity's own information.

- 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
- 32
- 33
- 34
- (3) An entity is liable to a civil penalty if:
- (a) the entity contravenes subsection (1); and
- (b) the entity is not:
- (i) a Commonwealth officer (within the meaning of Part 5.6 of the *Criminal Code*); or
- (ii) an officer or employee of a State body (within the meaning of the *Cyber Security Act 2024*); and
- (c) any of the following applies:
- (i) the information is sensitive information (within the meaning of the *Privacy Act 1988*) about a person and the person has not consented to the record, use or communication of the information;
- (ii) the information is confidential or commercially sensitive;
- (iii) the record, use or communication of the information would, or could reasonably be expected to cause, damage to the security, defence or international relations of the Commonwealth.
- Note 1: See the *Criminal Code* for offences for Commonwealth officers.
- Note 2: This section does not make the Crown (other than an authority of the Crown) liable to a civil penalty.
- Note 3: For the application of provisions of the *Regulatory Powers (Standard Provisions) Act 2014* to this Division, see Part 6 of the *Cyber Security Act 2024*.
- Civil penalty: 50 penalty units.
- (4) This section binds the Crown in right of each of its capacities.
- (5) Subsection (4) does not make the Crown liable to be prosecuted for an offence.
- Note: The Crown (other than a Crown authority) is not liable to a pecuniary penalty for the breach of a civil penalty provision or to be given an infringement notice: see subsections 69(7) and 72(7) of the *Cyber Security Act 2024*.
- (6) The protection in subsection (5) does not apply to an authority of the Crown.

Schedule 1 Limited use of certain cyber security information

(7) This Division does not enable a power to be exercised to the extent that it would impair the capacity of a State to exercise its constitutional powers.

(8) For the purposes of this Division, *Commonwealth body* has the same meaning as in the *Cyber Security Act 2024*.

41BC Admissibility of information voluntarily given by impacted entity

(1) This section applies to information that:

- (a) is covered by subsection 41BA(2); and
- (b) has been voluntarily provided to ASD by an entity (the *impacted entity*), or on behalf of the impacted entity, as referred to in subparagraph 41BA(2)(b)(i).

(2) The information is not admissible in evidence against the impacted entity in:

- (a) criminal proceedings for an offence against a Commonwealth law, other than:
 - (i) proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* (which deal with false or misleading information or documents) that relates to this Act; or
 - (ii) proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act; or
- (b) civil proceedings for a contravention of a civil penalty provision of a Commonwealth law, other than a civil penalty provision of this Division.

(3) This section does not limit or affect any right, privilege or immunity that the entity has, apart from this section, as a defendant in any proceedings.

41BD Director-General of ASD and staff members of ASD not compellable as witnesses

- (1) A person who is, or has been, the Director-General of ASD or a staff member of ASD:
- (a) is not obliged to comply with a subpoena or similar direction of a federal court to attend and answer questions relating to information covered by subsection 41BA(2); and
 - (b) is not compellable to give an expert opinion in any civil or criminal proceedings in a federal court in relation to information covered by subsection 41BA(2).
- (2) This section does not apply to a coronial inquiry.

41BE How this Division applies in relation to non-legal persons

How permissions and rights are conferred and exercised

- (1) If this Division purports to confer a permission or right on an entity that is not a legal person, the permission or right:
- (a) is conferred on each person who is an accountable person for the entity at the time the permission or right may be exercised; and
 - (b) may be exercised by:
 - (i) any person who is an accountable person for the entity at the time the permission or right may be exercised; or
 - (ii) any person who is authorised by a person referred to in subparagraph (i) to exercise the permission or right.

How obligations and duties are imposed and discharged

- (2) If this Division purports to impose an obligation or duty on an entity that is not a legal person, the obligation or duty:
- (a) is imposed on each person who is an accountable person for the entity at the time the obligation or duty arises or is in operation; and
 - (b) may be discharged by:

Schedule 1 Limited use of certain cyber security information

- 1 (i) any person who is an accountable person for the entity
- 2 at the time the obligation or duty arises or is in
- 3 operation; or
- 4 (ii) any person who is authorised by a person referred to in
- 5 subparagraph (i) to discharge the obligation or duty.

6 *How non-legal persons contravene this Division*

- 7 (3) A provision of this Division (including a civil penalty provision)
- 8 that is purportedly contravened by an entity that is not a legal
- 9 person is instead contravened by each accountable person for the
- 10 entity who:
- 11 (a) did the relevant act or made the relevant omission; or
- 12 (b) aided, abetted, counselled or procured the relevant act or
- 13 omission; or
- 14 (c) was in any way knowingly concerned in, or party to, the
- 15 relevant act or omission.

16 *Meaning of accountable person*

- 17 (4) For the purposes of this section, a person is an **accountable person**
- 18 for an entity at a particular time if:
- 19 (a) in the case of a partnership in which one or more of the
- 20 partners is an individual—the individual is a partner in the
- 21 partnership at that time; or
- 22 (b) in the case of a partnership in which one or more of the
- 23 partners is a body corporate—the person is a director of the
- 24 body corporate at that time; or
- 25 (c) in the case of a trust in which the trustee, or one or more of
- 26 the trustees, is an individual—the individual is a trustee of
- 27 the trust at that time; or
- 28 (d) in the case of a trust in which the trustee, or one or more of
- 29 the trustees, is a body corporate—the person is a director of
- 30 the body corporate at that time; or
- 31 (e) in the case of an unincorporated association—the person is a
- 32 member of the governing body of the unincorporated
- 33 association at that time.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 41BF Contravening a civil penalty provision of this Division**

(1) This section applies if a provision of this Division provides that a person contravening another provision of this Division (the **conduct provision**) is liable to a civil penalty.

(2) For the purposes of this Division, and the *Regulatory Powers (Standard Provisions) Act 2014* to the extent that it relates to this Division, a reference to a contravention of a civil penalty provision includes a reference to a contravention of the conduct provision.

Note: For the application of provisions of the *Regulatory Powers (Standard Provisions) Act 2014* to this Division, see Part 6 of the *Cyber Security Act 2024*.

2022-2023-2024

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES/THE SENATE

EXPOSURE DRAFT

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

No. , 2024

(Home Affairs)

**A Bill for an Act to amend the law relating to
critical infrastructure and telecommunications, and
for related purposes**

Released by Department of Home Affairs
under the Freedom of Information Act 1982

EXPOSURE DRAFT

Contents

1	Short title	1
2	Commencement	1
3	Schedules	2
Schedule 1—Data storage systems that hold business critical data		4
	<i>Security of Critical Infrastructure Act 2018</i>	4
Schedule 2—Managing consequences of impacts of incidents on critical infrastructure assets		6
	<i>Security of Critical Infrastructure Act 2018</i>	6
Schedule 3—Use and disclosure of protected information		13
	<i>Security of Critical Infrastructure Act 2018</i>	13
Schedule 4—Direction to vary critical infrastructure risk management program		21
	<i>Security of Critical Infrastructure Act 2018</i>	21
Schedule 5—Security regulation for the telecommunications sector		25
Part 1—Main amendments		25
	<i>Security of Critical Infrastructure Act 2018</i>	25
Part 2—Consequential amendments		38
	<i>Australian Security Intelligence Organisation Act 1979</i>	38
	<i>Telecommunications Act 1997</i>	38
	<i>Telecommunications (Interception and Access) Act 1979</i>	42
Part 3—Application and saving provisions		43
Schedule 6—Notification of declaration of system of national significance		44
	<i>Security of Critical Infrastructure Act 2018</i>	44

1 **A Bill for an Act to amend the law relating to**
2 **critical infrastructure and telecommunications, and**
3 **for related purposes**

4 The Parliament of Australia enacts:

5 **1 Short title**

6 This Act is the *Security of Critical Infrastructure and Other*
7 *Legislation Amendment (Enhanced Response and Prevention) Act*
8 2024.

9 **2 Commencement**

10 (1) Each provision of this Act specified in column 1 of the table
11 commences, or is taken to have commenced, in accordance with

No.	, 2024	<i>Security of Critical Infrastructure and Other Legislation Amendment</i> <i>(Enhanced Response and Prevention) Bill 2024</i>	1
-----	--------	---	---

1 column 2 of the table. Any other statement in column 2 has effect
2 according to its terms.

3

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. Schedules 1 to 4	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 6 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	
3. Schedule 5	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.	
4. Schedule 6	At the same time as the provisions covered by table item 2.	

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

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

10 **3 Schedules**

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

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

No. , 2024 *Security of Critical Infrastructure and Other Legislation Amendment* 3
(Enhanced Response and Prevention) Bill 2024

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Schedule 1—Data storage systems that hold business critical data

Security of Critical Infrastructure Act 2018

1 Subsection 9(1) (note)

Omit “Note”, substitute “Note 1”.

2 At the end of subsection 9(1)

Add:

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

3 At the end of section 9

Add:

Data storage systems

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

- (a) the data storage system is used, or is to be used, in connection with the critical infrastructure asset;
- (b) business critical data is stored, or is processed in or by, the data storage system (whether or not other information is also stored, or is processed in or by, the data storage system);
- (c) for a hazard where there is a material risk that the occurrence of the hazard could have an impact on the data storage system, there is also a material risk that the occurrence of the hazard could have a relevant impact on the critical infrastructure asset.

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

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

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- (b) a critical infrastructure risk management program under Part 2A in relation to a critical infrastructure asset will also need to cover the data storage system; and
- (c) notification obligations under Part 2B of cyber security incidents relating to any relevant impact on a critical infrastructure asset will also need to take into account any relevant impact on the data storage system.

8

4 Application provision

9

10

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

- 11
- 12
- 13
- 14
- 15
- 16
- (a) assets that are critical infrastructure assets (including systems of national significance) immediately before the commencement of this item;
- (b) assets that become critical infrastructure assets (including systems of national significance) on or after the day on which this item commences;

17

18

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

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

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

Security of Critical Infrastructure Act 2018

1 Paragraph 3(e)

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

2 Section 4

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

3 Subsections 8G(2) and (3)

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

4 Section 12P (heading)

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

5 Section 12P

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

6 Part 3A (heading)

Repeal the heading, substitute:

Part 3A—Responding to serious incidents

7 Section 35AA

Repeal the section, substitute:

35AA Simplified outline of this Part

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

8 Division 2 of Part 3A (heading)

Repeal the heading, substitute:

Division 2—Ministerial authorisation relating to serious incidents

9 Paragraph 35AB(1)(a)

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

EXPOSURE DRAFT

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

10 Paragraph 35AB(1)(b)

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

11 Paragraph 35AB(1A)(a)

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

12 Paragraph 35AB(1A)(b)

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

13 Paragraph 35AB(2)(a)

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

14 Paragraph 35AB(2)(b)

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

15 Paragraph 35AB(2)(c)

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

16 Paragraph 35AB(2)(d)

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

17 Paragraph 35AB(2)(e)

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

18 Paragraph 35AB(2)(f)

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

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

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

20 Paragraph 35AB(5)(a)

After “the asset”, insert “or assets”.

21 Subsection 35AB(7)

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

22 Subsection 35AB(7) (note)

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

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

After “the asset”, insert “or assets”.

24 Subsection 35AB(9)

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

25 After subsection 35AB(9)

Insert:

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

1 (9A) Without limiting paragraph (2)(c) or (d), a direction referred to in
2 that paragraph may require a specified entity to disclose specified
3 personal information (within the meaning of the *Privacy Act 1988*)
4 held by the entity to another specified entity for a specified
5 purpose.

6 (9B) However, the Minister must not give a Ministerial authorisation
7 under paragraph (2)(c) or (d), to the extent that it authorises the
8 giving of a direction covered by subsection (9A), unless the
9 Minister has obtained the agreement of the Minister administering
10 the *Privacy Act 1988*.

11 **26 Subsection 35AB(10)**

12 After “paragraph (2)(e) or (f)”, insert “that relates to the incident and an
13 asset”.

14 **27 Before paragraph 35AB(10)(a)**

15 Insert:
16 (aa) the incident is a cyber security incident; and

17 **28 Paragraphs 35AB(10)(b) and (c)**

18 Omit “concerned”.

19 **29 Paragraph 35AB(11)(a)**

20 Omit “concerned”.

21 **30 Section 35AC**

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

25 **31 Paragraphs 35AC(a) to (j)**

26 Omit “to which the Ministerial authorisation relates” (wherever
27 occurring).

28 **32 Subsection 35AD(1)**

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

EXPOSURE DRAFT

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

Document 5

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

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

34 Paragraph 35AF(2)(a)

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

35 Paragraph 35AG(1)(a)

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

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

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

37 Paragraph 35AK(1)(a)

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

38 Subsection 35AQ(2) (note)

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

39 Subsection 35AS(3)

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

40 Subsection 35AX(2) (note)

Omit “section 35AB”, substitute “subsection 35AB(10)”.

41 At the end of subsection 35BA(1)

Add “and an asset”.

42 Subsection 35BK(1)

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

43 Application and saving provisions

- (1) The amendments of Part 3A of the *Security of Critical Infrastructure Act 2018* made by this Schedule apply in relation to the giving of an

No. , 2024 *Security of Critical Infrastructure and Other Legislation Amendment
(Enhanced Response and Prevention) Bill 2024* 11

Released by Department of Home Affairs
under the Freedom of Information Act 1982

EXPOSURE DRAFT

EXPOSURE DRAFT

Document 5

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

-
- 1 authorisation under subsection 35AB(2) of that Act on or after the day
2 on which this item commences in relation to an application by the
3 Secretary under that subsection on or after that day.
- 4 (2) The *Security of Critical Infrastructure Act 2018*, as in force
5 immediately before the commencement of this item, continues to apply
6 on and after that commencement in relation to the following:
- 7 (a) an authorisation given under subsection 35AB(2) of that Act
8 before the day on which this item commences;
- 9 (b) an application by the Secretary under that subsection before
10 that day.

12 *Security of Critical Infrastructure and Other Legislation Amendment* No. , 2024
(*Enhanced Response and Prevention*) Bill 2024

EXPOSURE DRAFT

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Schedule 3—Use and disclosure of protected information

Security of Critical Infrastructure Act 2018

1 Section 4

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

2 Section 5

Insert:

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

confidential commercial information means the following:

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

3 Section 5 (definition of *protected information*)

Repeal the definition, substitute:

protected information has the meaning given by section 5A.

4 Section 5

Insert:

relevant information has the meaning given by section 5A.

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

Repeal the paragraph, substitute:

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

3 **6 Section 5 (paragraph (b) of the definition of security)**

4 Omit “definition of *critical energy market operator asset*”, substitute
5 “definitions of *critical energy market operator asset* and *protected*
6 *information*”.

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

8 Omit “and 30CW”, substitute “, 30CW and 42AA”.

9 **8 After section 5**

10 Insert:

11 **5A Meaning of *protected information* and *relevant information***

12 *Protected information*

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

- 14 (a) the disclosure of which would or could reasonably be
15 expected to prejudice national security or the defence of
16 Australia; or
17 (b) the disclosure of which would or could reasonably be
18 expected to prejudice the social or economic stability of
19 Australia or its people; or
20 (c) that contains, or is, confidential commercial information; or
21 (d) the disclosure of which would or could reasonably be
22 expected to prejudice the availability, integrity, reliability or
23 security of a critical infrastructure asset.

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

- 25 (a) was a document or information to which subsection (1)
26 applied; and
27 (b) is obtained by a person by way of an authorised disclosure
28 under Division 3 of Part 4 or in accordance with section 46.

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

- (a) a document or information that is obtained or generated by a person in the course of exercising powers, or performing duties or functions, under this Act; or
 - (b) a document or information that is obtained, generated or adopted by an entity for the purposes of complying with this Act;
- including, but not limited to, a document or information that:
- (c) records or is the fact that an asset is declared under section 51 to be a critical infrastructure asset; or
 - (d) records or is the fact that an asset is declared under section 52B to be a system of national significance; or
 - (e) records or is the fact that the Minister has:
 - (i) given a Ministerial authorisation; or
 - (ii) revoked a Ministerial authorisation; or
 - (f) is, or is included in, a critical infrastructure risk management program that is adopted by an entity in compliance with section 30AC; or
 - (g) is, or is included in, a report that is given under section 30AG or 30AQ; or
 - (h) is, or is included in, a report under section 30BC or 30BD; or
 - (i) is, or is included in, an incident response plan adopted by an entity in compliance with section 30CD; or
 - (j) is, or is included in, an evaluation report prepared under section 30CQ or 30CR; or
 - (k) is, or is included in, a vulnerability assessment report prepared under section 30CZ; or
 - (l) is, or is included in, a report prepared in compliance with:
 - (i) a system information periodic reporting notice; or
 - (ii) a system information event-based reporting notice; or
 - (m) records or is the fact that the Secretary has:
 - (i) given a direction under section 35AK; or
 - (ii) revoked such a direction; or
 - (n) records or is the fact that the Secretary has:

Schedule 3 Use and disclosure of protected information

- 1 (i) given a direction under section 35AQ; or
2 (ii) revoked such a direction; or
3 (o) records or is the fact that the Secretary has:
4 (i) given a request under section 35AX; or
5 (ii) revoked such a request.

6 **9 Section 36 (note)**

7 Omit “section 5”, substitute “section 5A”.

8 **10 Subsections 42(1) and (2)**

9 After “Secretary”, insert “, or an authorised APS employee,”.

10 **11 After subparagraph 42(2)(a)(vii)**

11 Insert:

12 (viiia) emergency management;

13 **12 Paragraph 42(2)(b)**

14 Repeal the paragraph, substitute:

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

22 **13 At the end of section 42**

23 Add:

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

28 **14 After section 42**

29 Insert:

1 **42AA Authorised use and disclosure—availability, integrity,**
2 **reliability or security of a critical infrastructure asset**

3 An entity may make a record of, use or disclose protected
4 information if the entity makes the record, or uses or discloses the
5 information:

- 6 (a) for a purpose relating to the continued operation of a critical
7 infrastructure asset; or
8 (b) to mitigate a risk to the availability, integrity, reliability or
9 security of a critical infrastructure asset.

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

12 **15 Section 42A**

13 Before “The”, insert “(1)”.

14 **16 Section 42A**

15 After “Secretary”, insert “, or an authorised APS employee,”.

16 **17 At the end of section 42A**

17 Add:

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

22 **18 Section 43**

23 Before “The”, insert “(1)”.

24 **19 Section 43**

25 After “Secretary”, insert “, or an authorised APS employee,”.

26 **20 At the end of section 43**

27 Add:

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

4 **21 Section 43AA**

5 Before “The”, insert “(1)”.

6 **22 Section 43AA**

7 After “Secretary”, insert “, or an authorised APS employee,”.

8 **23 At the end of section 43AA**

9 Add:

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

14 **24 Section 43A**

15 Before “The”, insert “(1)”.

16 **25 Section 43A**

17 After “Secretary”, insert “, an authorised APS employee or any other
18 entity”.

19 **26 At the end of section 43A**

20 Add:

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

25 **27 Subparagraphs 43E(1)(b)(i) and (ii)**

26 After “responsibility for”, insert “emergency management or for”.

27 **28 Subsections 43E(2) and (3)**

28 Repeal the subsections, substitute:

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

7 Note: This subsection is an authorisation for the purposes of other laws,

8 including the Australian Privacy Principles.

9 **29 After section 43E**

10 Insert:

11 **43F Authorised use and disclosure—entity's business, professional,**

12 **commercial or financial affairs**

13 An entity may make a record of, use or disclose protected

14 information if:

- 15 (a) the protected information was obtained, generated or adopted
- 16 by the entity for the purposes of complying with this Act; and
- 17 (b) the entity makes the record, or uses or discloses the
- 18 information for the entity's business, professional,
- 19 commercial or financial affairs.

20 Note: This section is an authorisation for the purposes of other laws,

21 including the Australian Privacy Principles.

22 **30 At the end of Subdivision A of Division 3 of Part 4**

23 Add:

24 **44A Authorised APS employees**

- 25 (1) The Secretary may, in writing, authorise an APS employee in the
- 26 Department, or each APS employee in the Department included in
- 27 a specified class of APS employees in the Department, to be an
- 28 authorised APS employee for the purposes of this Subdivision.
- 29 (2) The Secretary must, in any authorisation under subsection (1),
- 30 specify the kind of protected information that the APS employee,
- 31 or each APS employee in that class, is authorised:

Schedule 3 Use and disclosure of protected information

- 1 (a) to disclose under section 42, 42A, 43, 43AA or 43A; and
2 (b) to make a record of or use for the purpose of a disclosure
3 under section 42, 42A, 43AA or 43A.

31 Paragraph 45(1)(a)

- 4 Repeal the paragraph, substitute:
5 (a) the entity obtains, generates or adopts a document or
6 information; and
7

32 Paragraph 45(1)(b)

- 8 After “the”, insert “document or”.

33 Paragraph 45(1)(c)

- 10 After “uses the”, insert “document or”.

34 Subsection 45(1) (note 2)

- 12 Repeal the note, substitute:
13 Note 2: A document or information that records or is the fact that an asset is
14 declared under section 51 to be a critical infrastructure asset may be
15 protected information: see section 5A.
16

35 Application provision

- 17 The amendments of the *Security of Critical Infrastructure Act 2018*
18 made by this Schedule apply in relation to the making of a record, use
19 or disclosure of a document or information on or after the day on which
20 this item commences, whether the document or information is obtained,
21 generated or adopted before, on or after that day.
22

**Schedule 4—Direction to vary critical
infrastructure risk management
program**

Security of Critical Infrastructure Act 2018

1 Section 5

Insert:

relevant official has the meaning given by section 30AI.

serious deficiency has the meaning given by section 30AI.

2 Before paragraph 30AG(2)(e)

Insert:

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

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

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

3 After section 30AH

Insert:

**30AI Direction to vary critical infrastructure risk management
program**

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

(2) The *relevant official* is:

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

Schedule 4 Direction to vary critical infrastructure risk management program

- 1 (b) if there is a relevant Commonwealth regulator that has
2 functions relating to the security of those assets:
3 (i) the chief executive officer (however described) of that
4 regulator; or
5 (ii) an SES employee, or an acting SES employee, in that
6 regulator; or
7 (iii) a person who holds, or is acting in, a position in that
8 regulator that is equivalent to, or higher than, a position
9 occupied by an SES employee in the Department.

- 10 (3) A **serious deficiency** is a deficiency that poses a material risk to:
11 (a) national security; or
12 (b) the defence of Australia; or
13 (c) the social or economic stability of Australia or its people.

14 *Contents of direction*

- 15 (4) A direction under subsection (1) must:
16 (a) specify the serious deficiencies; and
17 (b) require the responsible entity to vary the entity’s critical
18 infrastructure risk management program to address those
19 deficiencies; and
20 (c) specify the period within which the responsible entity must
21 vary that program, which must be a period of at least 14 days
22 starting on the day on which the direction is given.

23 *Compliance with direction*

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

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

27 Civil penalty: 250 penalty units.

28 *Consultation before giving direction*

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

EXPOSURE DRAFT

Direction to vary critical infrastructure risk management program **Schedule 4**

- 1 (a) stating that the relevant official is considering giving the
2 responsible entity a direction under subsection (1); and
3 (b) specifying the serious deficiencies covered by subsection (1);
4 and
5 (c) invite the responsible entity to give the relevant official,
6 within 14 days after the day the notice is given to the
7 responsible entity, a written submission in relation to the
8 notice.
- 9 (7) The relevant official must, in deciding whether to give a direction
10 under subsection (1), have regard to:
11 (a) any written submission received from the responsible entity
12 within that 14-day period; and
13 (b) any action that is taken, or proposed to be taken, by the
14 responsible entity in response to the notice and that is
15 notified to the relevant official within that 14-day period.
- 16 (8) Subsection (7) does not limit the matters to which the relevant
17 official may have regard.
- 18 *Head of relevant Commonwealth regulator to give copy of*
19 *direction to Secretary*
- 20 (9) If the head (however described) of a relevant Commonwealth
21 regulator gives a direction under subsection (1), the head must give
22 the Secretary a copy of the direction.
- 23 *Direction not a legislative instrument*
- 24 (10) A direction under subsection (1) is not a legislative instrument.

4 After paragraph 60(2)(g)

26 Insert:

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

EXPOSURE DRAFT

Schedule 4 Direction to vary critical infrastructure risk management program

5 Application provisions

- (1) The amendments of sections 30AG and 60 of the *Security of Critical Infrastructure Act 2018* made by this Schedule apply in relation to a financial year that ends after the day on which this item commences.
- (2) Section 30AI of the *Security of Critical Infrastructure Act 2018*, as inserted by this Schedule, applies in relation to a direction given on or after the day on which this item commences, whether the critical infrastructure risk management program was adopted before, on or after that day.

24 Security of Critical Infrastructure and Other Legislation Amendment No. , 2024
 (Enhanced Response and Prevention) Bill 2024

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

EXPOSURE DRAFT

1 **Schedule 5—Security regulation for the**
2 **telecommunications sector**

3 **Part 1—Main amendments**

4 *Security of Critical Infrastructure Act 2018*

5 **1 After paragraph 3(d)**

6 Insert:
7 (da) imposing enhanced security obligations on responsible
8 entities for critical telecommunications assets; and

9 **2 Section 4**

10 After:

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

13 insert:

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

16 **3 Section 5 (note to the definition of *critical public transport***
17 ***asset*)**

18 Omit “Note”, substitute “Note 1”.

19 **4 Section 5 (at the end of the definition of *critical public***
20 ***transport asset*)**

21 Add:

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

24 **5 Section 5 (paragraph (b) of the definition of *critical***
25 ***telecommunications asset*)**

26 Repeal the paragraph, substitute:

Schedule 5 Security regulation for the telecommunications sector
Part 1 Main amendments

- (b) any other asset:
 - (i) that is owned or operated by a carrier or a carriage service provider; and
 - (ii) that is used in connection with the supply of a carriage service.

6 Section 5

Insert:

notifiable equipment has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.
satellite-based facility has the same meaning as in the *Telecommunications Act 1997*.

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

Omit “Note”, substitute “Note 1”.

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

Add:

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

9 Section 5

Insert:

submarine cable has the same meaning as it has in Schedule 3A to the *Telecommunications Act 1997*.
telecommunications service has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.
telecommunications system has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

- 1
2
3
- unauthorised*, in relation to access, modification or impairment of
a kind mentioned in subsection 12N(1), has the meaning given by
section 12N.
- 4
5
6
- 10 Section 5 (definition of *unauthorised access, modification or impairment*)**
Repeal the definition.
- 7
8
- 11 After subsection 9(2B)**
Insert:
- 9
10
11
- (2C) However, subsection (2B) does not apply for the purposes of
working out whether a satellite-based facility or submarine cable is
a critical telecommunications asset.
- 12
13
14
15
- Note: Section 14 provides that this Act applies both within and outside
Australia. The effect of subsection (2C) of this section and section 14
is that a satellite-based facility or submarine cable located outside
Australia may be a critical telecommunications asset.
- 16
17
- 12 Subsection 10(1) (note)**
Omit “Note”, substitute “Note 1”.
- 18
19
- 13 At the end of subsection 10(1)**
Add:
- 20
21
- Note 2: A critical electricity asset that is owned or operated by a carrier may
also be a critical telecommunications asset.
- 22
23
- 14 Subsection 12B(1) (note)**
Omit “Note”, substitute “Note 1”.
- 24
25
- 15 At the end of subsection 12B(1)**
Add:
- 26
27
- Note 2: A critical freight infrastructure asset that is owned or operated by a
carrier may also be a critical telecommunications asset.
- 28
29
- 16 Subsection 12C(1) (note)**
Omit “Note”, substitute “Note 1”.

Schedule 5 Security regulation for the telecommunications sector
Part 1 Main amendments

17 At the end of subsection 12C(1)

Add:

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

18 Subsection 12F(1) (note)

Omit “Note”, substitute “Note 1”.

19 At the end of subsection 12F(1)

Add:

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

20 Subsection 12F(2) (note)

Omit “Note”, substitute “Note 1”.

21 At the end of subsection 12F(2)

Add:

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

22 Subsection 12N(1)

Omit “unauthorised”, substitute “*unauthorised*”.

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

Insert:

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

24 After paragraph 30AG(2)(d)

Insert:

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

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- (i) includes a summary of the changes (if any) the entity notified during the relevant period under subsection 30EC(2); and
- (ii) describes the risks (if any) advised to the entity during the relevant period under paragraph 30ED(3)(c); and
- (iii) describes the measures (if any) the entity adopted during the relevant period to eliminate or reduce risks advised to the entity during the relevant period or any previous period; and
- (iv) includes a statement that evaluates the effectiveness of those measures to eliminate or reduce risks advised to the entity during the relevant period or any previous period; and

14

25 After Part 2C

15

Insert:

16

Part 2D—Enhanced security regulation for critical

17

telecommunications assets

18

Division 1—Introduction

19

30EA Simplified outline of this Part

20

21

22

23

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

- 24
- 25
- 26
- 27
- (a) security; and
- (b) the protection of the asset from any hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset.

28

29

30

31

The responsible entity for a critical telecommunications asset that is prescribed by the rules must notify the Secretary of certain changes, and proposed changes, to telecommunications services or telecommunications systems if the change, or proposed change, is

likely to have a material adverse effect on the entity’s capacity to comply with the obligation to protect the asset for the purposes of security.

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

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

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

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

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

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

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

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

Civil penalty: 1,500 penalty units.

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

- 1 (a) any requirements that apply to the entity and the asset under
2 Part 2A (critical infrastructure risk management programs);
3 (b) the requirement to maintain competent supervision of, and
4 effective control over, the asset;
5 (c) any other requirements prescribed by the rules for the
6 purposes of this paragraph.
- 7 (4) An entity is not liable to an action or other proceeding for damages
8 for or in relation to an act done or omitted in good faith in
9 performance of the obligation imposed by subsection (2).
- 10 (5) An officer, employee or agent of an entity is not liable to an action
11 or other proceeding for damages for or in relation to an act done or
12 omitted in good faith in connection with an act done or omitted by
13 the entity as mentioned in subsection (4).

14 **Division 3—Responsible entity’s notification obligations**
15 **impacting their security obligations**

16 **30EC Responsible entity to notify certain changes and proposed**
17 **changes to telecommunications service or system**

- 18 (1) This section applies if, at any time, the responsible entity for a
19 critical telecommunications asset prescribed by the rules for the
20 purposes of this subsection becomes aware that the implementation
21 of a change, or proposed change, by the entity to:
22 (a) a telecommunications service; or
23 (b) a telecommunications system;
24 is likely to have a material adverse effect on the entity’s capacity to
25 comply with its obligation under subsection 30EB(2), to the extent
26 that subsection applies for the purposes of security and the asset.
- 27 Note 1: For specification by class, see subsection 13(3) of the *Legislation Act*
28 *2003*.
- 29 Note 2: See section 30EE for the kinds of changes covered by this Division.
- 30 (2) As soon as reasonably practicable after becoming aware that the
31 change, or proposed change, is likely to have a material adverse
32 effect as mentioned in subsection (1), the responsible entity for the
33 critical telecommunications asset must:

Schedule 5 Security regulation for the telecommunications sector
Part 1 Main amendments

- 1 (a) notify the Secretary, in writing, of the change, or of the
2 entity's intention to implement the proposed change; and
3 (b) specify the asset in the notification; and
4 (c) include in the notification a description of the change or
5 proposed change; and
6 (d) in relation to the change or proposed change—include in the
7 notification any other information of a kind prescribed by the
8 rules for the purposes of this paragraph.

9 Civil penalty: 300 penalty units.

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

14 *Further information*

- 15 (4) If:
16 (a) the responsible entity for a critical telecommunications asset
17 gives a notification under subsection (2) in relation to a
18 change or proposed change; and
19 (b) the Secretary considers that further information is required
20 for the Secretary to assess whether, in relation to the change
21 or proposed change, there is a risk of unauthorised
22 interference with, or unauthorised access to, the asset that
23 would be prejudicial to security;
24 the Secretary may, by written notice given to the entity, require the
25 entity to give the Secretary specified further information by the end
26 of:
27 (c) 44 business days after the day the notice is given; or
28 (d) such longer period as the Secretary allows.
- 29 (5) The Secretary must give any notice under subsection (4) by the end
30 of 22 business days after the day the Secretary receives the
31 notification under subsection (2).
- 32 (6) If the Secretary:
33 (a) gives a notice to the entity under subsection (4) in relation to
34 specified further information; and

(b) considers that information additional to the specified further information is required for the Secretary to make the assessment mentioned in paragraph (4)(b);
the Secretary may give the entity a further notice under subsection (4) in relation to the additional further information.
Subsection (5) does not apply to the further notice.

Compliance with notice

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

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

Civil penalty: 150 penalty units.

Self-incrimination

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

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

- (a) the information given; or
 - (b) giving the information; or
 - (c) any information, document or thing obtained as a direct or indirect consequence of giving the information;
- is not admissible in evidence against the individual:
- (d) in criminal proceedings other than proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* that relates to this Act; or
 - (e) in civil proceedings other than proceedings for recovery of a penalty in relation to a contravention of subsection (7) of this section.

30ED Secretary to assess notified changes and proposed changes

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

Schedule 5 Security regulation for the telecommunications sector
Part 1 Main amendments

- 1 (2) The Secretary must give the entity a notice under subsection (3) or
2 (4) of this section:
 - 3 (a) by the end of 22 business days after the day the Secretary
4 receives the notification, unless paragraph (b) of this
5 subsection applies; or
 - 6 (b) if the Secretary sought further information from the entity by
7 one or more notices given under subsection 30EC(4)—as
8 soon as practicable, and no later than 22 business days, after
9 the day the entity provided the information sought by the last
10 notice given under that subsection.
- 11 (3) If:
 - 12 (a) the Secretary considers the change or proposed change
13 (including where further information is provided in response
14 to a notice given under subsection 30EC(4)); and
 - 15 (b) in relation to the change or proposed change, the Secretary is
16 satisfied that there is a risk of unauthorised interference with,
17 or unauthorised access to, the asset that would be prejudicial
18 to security;the Secretary:
 - 19 (c) must give a written notice to the entity:
 - 20 (i) advising the entity of that risk; and
 - 21 (ii) setting out the entity's obligation under
22 subsection 30EB(2); and
 - 23 (iii) setting out the consequences for the entity for not
24 complying with that obligation; and
 - 25 (d) may set out in that notice the measures the Secretary
26 considers the entity could adopt to eliminate or reduce that
27 risk.
28
- 29 (4) If:
 - 30 (a) the Secretary considers the change or proposed change
31 (including where further information is provided in response
32 to a notice given under subsection 30EC(4)); and
 - 33 (b) in relation to the change or proposed change, the Secretary is
34 satisfied that there is not a risk of unauthorised interference
35 with, or unauthorised access to, that asset that would be
36 prejudicial to security;

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

2 **30EE Kinds of changes and proposed changes to**
3 **telecommunications services or telecommunications**
4 **systems**

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

- 8 (a) the responsible entity concerned providing one or more new
9 telecommunication services;
- 10 (b) the responsible entity concerned changing the location of
11 notifiable equipment (including moving equipment outside
12 Australia);
- 13 (c) the responsible entity concerned procuring notifiable
14 equipment (including procuring equipment that is located
15 outside Australia);
- 16 (d) the responsible entity concerned entering into outsourcing
17 arrangements:
- 18 (i) to have all or part of the telecommunication services
19 provided for that entity; or
- 20 (ii) to have all or part of the provision of telecommunication
21 services managed for that entity; or
- 22 (iii) to have all or some information to which section 276 of
23 the *Telecommunications Act 1997* applies in relation to
24 that entity, managed for that entity;
- 25 (e) the responsible entity concerned entering into arrangements
26 to have all or some information to which section 276 of the
27 *Telecommunications Act 1997* applies in relation to that
28 entity accessed by persons outside Australia;
- 29 (f) the responsible entity concerned entering into arrangements
30 to have all or some information or documents to which
31 subsection 187A(1) of the *Telecommunications (Interception*
32 *and Access) Act 1979* applies in relation to that entity kept
33 outside Australia.

34 (2) This Division does not apply to changes or proposed changes to a
35 telecommunications service or a telecommunications system that

Schedule 5 Security regulation for the telecommunications sector
Part 1 Main amendments

1 are changes, or proposed changes, determined in an instrument
2 under subsection (3).

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

5 **Division 4—Ministerial directions**

6 **30EF Minister’s direction if use or supply of carriage services**
7 **prejudicial to security**

8 (1) If:

9 (a) the responsible entity for a critical telecommunications asset
10 proposes to use, or uses, for the entity’s own requirements or
11 benefit, or proposes to supply, or supplies, to another person,
12 one or more carriage services; and

13 (b) the Minister considers that the proposed use or supply would
14 be, or the use or supply is, as the case may be, prejudicial to
15 security;

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

19 (2) A direction under subsection (1) must:

20 (a) relate to a carriage service generally and cannot be expressed
21 to apply to the supply of a carriage service to a particular
22 person, particular persons or a particular class of persons; or

23 (b) specify the period within which the entity must comply with
24 the direction (which must be a period that is reasonable in the
25 circumstances).

26 *Direction to be given after adverse security assessment*

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

Security regulation for the telecommunications sector **Schedule 5**
Main amendments **Part 1**

Main amendments **Part 1**

Part 2—Consequential amendments

Australian Security Intelligence Organisation Act 1979

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

Repeal the subparagraph.

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

After “subsection”, insert “30EF(1) or”.

29 Paragraph 38A(1)(b)

Repeal the paragraph.

30 Subsection 38A(1A)

After “section”, insert “30EF or”.

31 Subsection 38A(1A)

Omit “act or omission would be”, substitute “thing being”.

Telecommunications Act 1997

32 Section 5

Omit:

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

substitute:

EXPOSURE DRAFT

Document 5

Security regulation for the telecommunications sector **Schedule 5**
Consequential amendments **Part 2**

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

33 Section 311

Omit:

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

substitute:

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

34 Section 311

Omit:

- The Home Affairs Minister may give directions to a carrier or a carriage service provider in certain circumstances where certain activities may be prejudicial to security.

No. , 2024 *Security of Critical Infrastructure and Other Legislation Amendment* 39
(Enhanced Response and Prevention) Bill 2024

Released by Department of Home Affairs
under the Freedom of Information Act 1982

EXPOSURE DRAFT

EXPOSURE DRAFT

Schedule 5 Security regulation for the telecommunications sector
Part 2 Consequential amendments

- The Home Affairs Secretary may obtain information from carriers, carriage service providers and carriage service intermediaries if the information is relevant to assessing compliance with the duty of those persons to protect telecommunications networks and facilities from unauthorised interference or unauthorised access.

35 Subsection 312(1)

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

36 Subsection 313(1)

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

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

Repeal the subsections.

38 Subsection 313(2)

Omit “do the intermediary’s best to prevent”, substitute “prevent, so far as it is reasonably practicable to do so,”.

39 Subsection 313(2A)

Repeal the subsection.

40 Paragraph 313(5)(a)

Omit “(1A),”.

41 Paragraph 313(5)(a)

Omit “(2A),”.

42 Paragraph 313(5)(b)

Omit “312; or”, substitute “312.”.

43 Paragraph 313(5)(c)

Repeal the paragraph.

- 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
- 44 Divisions 3, 5, 6, 7, 8 and 8A of Part 14**

Repeal the Divisions.

45 Subsections 564(1) and (2)

Omit “, the ACCC or the Home Affairs Minister”, substitute “or the ACCC”.

46 Subsection 564(3A)

Repeal the subsection.

47 Subsection 571(1)

Omit “, the ACCC or the Home Affairs Minister”, substitute “or the ACCC”.

48 Subsection 571(4)

Repeal the subsection.

49 Section 572A

Omit “or the Home Affairs Minister”.

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

Omit “or the Home Affairs Minister”.

51 Subsection 572B(5)

Omit “The Home Affairs Minister may arrange for the publishing of the undertaking on the Home Affairs Department’s website.”.

52 Subsection 572B(5A)

Repeal the subsection.

53 Subsection 572B(5B)

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

54 Subsection 572C(1)

Omit “or the Home Affairs Minister” (wherever occurring).

EXPOSURE DRAFT

Schedule 5 Security regulation for the telecommunications sector

Part 2 Consequential amendments

55 Subsection 572C(3)

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

Telecommunications (Interception and Access) Act 1979

56 Subparagraph 202A(a)(ii)

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

57 Paragraph 202B(1)(b)

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

42 Security of Critical Infrastructure and Other Legislation Amendment No. , 2024
 (Enhanced Response and Prevention) Bill 2024

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

EXPOSURE DRAFT

EXPOSURE DRAFT

Security regulation for the telecommunications sector **Schedule 5**
Application and saving provisions **Part 3**

- 1
- Part 3—Application and saving provisions**
- 2
- [to be added later.]*

Schedule 6—Notification of declaration of system of national significance

Security of Critical Infrastructure Act 2018

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

Repeal the paragraphs, substitute:

(r) subsection 52B(3).

2 Section 52A

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

3 Section 52A

Omit:

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

substitute:

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

4 Paragraph 52B(3)(a)

Repeal the paragraph, substitute:

(a) the responsible entity for the asset;

5 Section 52D

Repeal the section, substitute:

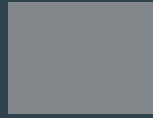
52D Notification if responsible entity for an asset ceases to be the responsible entity

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

Civil penalty: 150 penalty units.

6 Application and savings provisions

- (1) The amendment of section 52B of the *Security of Critical Infrastructure Act 2018* made by this Schedule applies in relation to a declaration made under subsection 52B(1) of that Act on or after the day on which this item commences.
- (2) Section 52D of the *Security of Critical Infrastructure Act 2018*, as substituted by this Schedule, applies in relation to a cessation that occurs on or after the day on which this item commences.
- (3) The *Security of Critical Infrastructure Act 2018*, as in force immediately before the commencement of this item, continues to apply on and after that commencement in relation to a matter referred to in paragraph 52D(1)(a) or (b) of that Act that occurred before that commencement.



Australian Government
Department of Home Affairs

Cyber Security Legislative Reforms Exposure Draft Paper

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

Released by Department of Home Affairs
under the Freedom of Information Act 1982

© Commonwealth of Australia 2023

With the exception of the Commonwealth Coat of Arms, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license at <https://creativecommons.org/licenses/by/4.0/legalcode>.



This means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website at <https://creativecommons.org/> as is the full legal code for the CC BY 4.0 license at <https://creativecommons.org/licenses/by/4.0/legalcode>.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed at the Department of the Prime Minister and Cabinet website—<https://www.pmc.gov.au/government/commonwealth-coat-arms>.

Contact us

Enquiries regarding the licence and any use of this document are welcome at:
Department of Home Affairs

PO Box 25

BELCONNEN ACT

2616 P - 23-02503-c

Table of Contents

Context of the Bill 2

Consultation 3

Part 1—Data storage systems that hold business critical data 4

Part 2—Managing consequences of impacts of incidents on critical infrastructure assets 5

Part 3—Use and disclosure of protected information 7

Part 4—Direction to vary critical infrastructure risk management program 8

Part 5—Security regulation for the telecommunications sector 9

Part 6—Notification of declaration of system of national significance 11

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

Context of the Bill

The Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (the Bill) would amend the *Security of Critical Infrastructure Act 2018* (SOCI Act), to give effect to the legislative reforms outlined under Shield 4 of the 2023-2030 Australian Cyber Security Strategy.

This Explanatory Document describes the intended operation and effect of amendments contained within the Bill.

Australians rely on critical infrastructure to deliver the essential services crucial to our way of life. Australia's critical infrastructure ecosystem provides essential goods and services that underpin Australia's national security, defence, and socioeconomic stability. Australia currently faces heightened geopolitical and cyber threats, which means that our critical infrastructure is increasingly at risk. Cyber attacks on Australian critical infrastructure remain an ongoing reality and can be highly lucrative for malicious state actors and cybercriminals. Data breaches as well as other cyber incidents and interruptions are increasing in scale and frequency. The loss of personal data can cause significant harm to Australian citizens and businesses, and the theft of sensitive data can result in large-scale fraud, put strain on the economy, destabilise the financial sector and reduce consumer confidence in our digital goods and services.

Data is not the only target of threat actors; critical infrastructure entities are themselves valuable targets, as they provide essential services to support Australian life and business – including our electricity, water, health, transport, logistics and telecommunication networks. In the Australian Security Intelligence Organisation's 2022-23 Annual Report, the Director General wrote that “foreign powers will increase their efforts to conduct espionage, and target Australia's defence systems and critical infrastructure. This includes intelligence activities that could be used to support potential cyber-enabled sabotage or other disruptive actions in the future”.

While many cyber attacks are focused on exfiltration of data from corporate databases, there is also a risk of lateral transfer to operational technology or network infrastructure. Large-scale attacks on these systems could cause major outages of essential services, resulting in widespread disruption of the Australian economy and society. In extreme cases, outages of essential systems could lead to loss of life.

The Australian Government released the 2023-2030 Cyber Security Strategy. ‘Shield 4’ of the Strategy proposed measures to protect critical infrastructure from serious incidents.

Recent incidents impacting critical infrastructure highlight gaps within the regulatory framework set out in the SOCI Act, such as:

- (a) the need to consistently capture assets that support the primary functions of critical infrastructure;
- (b) the need to enable an agile, industry-led response to incidents with support from Government as reasonably necessary; and
- (c) the need to continue to enhance uplift in critical infrastructure security, particularly the telecommunications sector.

The 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper (Consultation Paper) was publicly released following the Cyber Security Strategy. Measures 5 to 9 of the Consultation Paper correspond with the amendments contained within the Bill. Specifically, the SOCI Act amendments aim to:

- (a) expand the definition of all types of critical infrastructure assets to include secondary assets which hold ‘business critical data’ that relates to the functioning of the primary asset;
- (b) facilitate the use of the ‘last resort’ directions power for the Secretary, when authorised by the Minister, for the purposes of managing both multi asset incidents and the consequences of serious incidents which could have, are having, or has had, a ‘relevant impact’ on one or more critical infrastructure assets;
- (c) clarify the operation of the secrecy and disclosure provisions—in particular to enable greater intra-government sharing of protected information and cross-industry collaboration and reduce unnecessary burden of these provisions on entities in the ordinary conduct of business;

- (d) create a directions power for the Secretary of the Department of Home Affairs or the relevant Commonwealth regulator exercisable where it has been identified a critical infrastructure risk management program is seriously deficient;
- (e) bring appropriate elements of the Telecommunications Sector Security Reforms (TSSR) administered by the Home Affairs portfolio, including security and notification obligations, from Part 14 of the *Telecommunications Act 1997* (Telecommunications Act) into the SOCI Act, with enhancements to align the regulatory frameworks and clarify telecommunications-specific obligations, including via delegated legislation as required.

The Bill also amends Part 6A of the SOCI Act to strengthen the integrity of information that Part in respect of an asset that is or becomes a system of national significance (SoNS). Notification of changes under Part 6A will be communicated to the responsible entity only (see section 12L of the SOCI Act, which sets out the responsible entity for different assets), with obligations relating to SoNS notification removed for direct interest holders.

Consultation

On 19 December 2023 the Minister released the Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper. Consultation remained open until 1 March 2024. Home Affairs received over 130 written submissions and stakeholders broadly supportive of the proposals with feedback focused on ensuring the measures achieve their intended outcomes. The measures in this Bill have taken into account feedback provided throughout this consultation process.

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

Part 1—Data storage systems that hold business critical data

Introductory comments

The amendments contained within this Part would implement Measure 5 of the 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper (Consultation Paper), dealing with the protection of data storage systems and business critical data.

Critical infrastructure entities are a natural target for cyber incident given their size, function and value. Over the last two years, Australia has seen a growing number of cyber incidents impacting non-operational data storage systems held by critical infrastructure entities. Recent cyber incidents that did not directly impact the essential functions of critical infrastructure, have demonstrated the risk to the non-operational systems that hold large quantities of data. This includes both personal information and other 'business critical data'.

The SOCI Act currently imposes positive security obligations on data storage and processing assets, where this is the primary function of the critical infrastructure asset. Currently, these obligations do not extend to the adequate protection of secondary systems operated by other classes of critical infrastructure assets that hold 'business critical data'.

The purpose of the amendments contained within this Part is to strengthen and standardise obligations across critical infrastructure assets by explicitly outlining certain data storage systems that hold business critical data do form part of a critical infrastructure asset, regardless of the asset's primary function. The intent of this Part is not to capture all non-operational systems that hold business critical data, only those where vulnerabilities could have a relevant impact on critical infrastructure. Examples of the types of systems this could capture include: data storage systems that hold business critical data where there is inadequate network segregation between IT and OT systems, or data storage systems that hold operational data such as network blueprints, encryption keys, algorithms, operational system code, and tactics, techniques and procedures.

The *Privacy Act 1988* (Privacy Act) remains the primary framework for the protection of personal information.

Summary of changes

This Part is intended to capture only data storage systems that hold business critical data, where vulnerabilities, impacts or access to these systems could have a relevant impact on critical infrastructure. To effect this there are two key amendments proposed to the SOCI Act: a note in section 9(1) and a new subsection, 9(7). The new note in subsection 9(1) of the SOCI Act would clarify that data storage systems storing or processing business critical data are part of the critical infrastructure asset, if those systems are captured by the new subsection 9(7) of the Bill. The new subsection 9(7) of the Bill would clarify that a data storage system is part of a critical infrastructure asset where:

- the data storage system is used in connection with the main asset;
- the system stores or processes business critical data;
- impacts to that system could have a relevant impact on the critical infrastructure asset.

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

Introductory comments

The amendments contained within this Part would implement Measure 6 of the Consultation Paper, dealing with improving our national response to the consequences of significant incidents.

Consequence management typically takes place in coordination with crisis management and is concerned with steps taken to mitigate the immediate consequences and ramifications of an incident, and includes matters such as restoring services and reducing spread. This includes managing cascading impacts beyond the primary asset to other critical infrastructure sector assets. The existing government assistance powers in Part 3A of the SOCI Act are mechanisms to assist with an immediate response to serious cyber security incidents that pose a material risk to Australia's national interests. These use of current Part 3A powers is limited to responding to a cyber security incident and resolving the technical factors of that incident.

The current limits for utilising a Part 3A powers neglects to adequately consider or address the current threat and risk environment, where an effective response must address non-cyber incidents and consequence management at the resolution of an incident. This includes physical incidents like terrorist attacks and natural incidents such as floods or bushfires. The amendments enable use of the framework in response to consequential incidents caused by attacks on critical infrastructure assets. For example, an electricity asset is taken offline due to a fire. As a consequence, hospitals, transport and telecommunications services are operating at limited capacity. The framework would now be available to respond to the incidents and their impacts across critical infrastructure sectors. For example, the Government could request information surrounding the incidents and direct entities to act in the most effective manner to restore service functionality.

The purpose of the amendments contained within this Part is to facilitate management of consequences stemming from an 'all-hazards' incident through the government assistance framework. An 'all-hazards' incident refers to any hazard, natural or man-made, that may impact the availability, integrity, reliability and confidentiality of the critical infrastructure asset. This would include cyber and information hazards, physical and natural hazards, personnel hazards, and supply chain hazards.

The proposed amendments are designed to operate within the existing framework in the SOCI Act and will facilitate the management of multi-asset incidents and their consequences, such as a contagion event, with a non-established or non-cyber cause. This would enable the Government to directly mitigate consequences to the broader Australian critical infrastructure ecosystem. In doing so, the powers would better achieve the objectives of the SOCI Act to enhance critical infrastructure security and mitigate risks to Australia's social and economic stability, national security, and defence.

By expanding the existing government assistance framework under Part 3A of the SOCI Act, this would ensure the powers are subject to both existing and new safeguards where relevant. The existing safeguards require, before authorising a direction, the Minister to be satisfied that:

- the incident has had, is having, or is likely to have, a 'relevant impact' (as defined in new section 8G) on a critical infrastructure asset (paragraph 35AB(1)(b));
- there is a material risk that the incident has seriously prejudiced, is serious prejudicing, or is likely to seriously prejudice the social or economic stability of Australia or its people, defence or national security (paragraph 35AB(1)(c)); and
- no other regulatory system of the Commonwealth, State or Territory could be used to provide a practical and effective response to the incident (paragraph 35AB(1)(d)).

The requirements for the Minister and Secretary to consult the specified entity before issuing an authorisation or direction are also retained as safeguards within section 35AD of the SOCI Act.

Additional safeguards will be introduced to ensure:

- Intervention requests would continue to be limited to cyber security incidents only. Intervention requests authorise the Australian Signals Directorate to do the types of things specified in section 35AC including to access or modify computers in order to resolve a cyber incident. It would not be proportionate in responding to non-cyber incidents like natural disasters.
- Any authorisation in relation to a direction to disclose personal information would require the agreement from the Minister responsible for administering the Privacy Act.

These safeguards would ensure the Government has the appropriate tools available to respond to and manage serious incidents and their consequences in collaboration with all levels of government and industry, while preventing and mitigating the impact of an incident on the functionality of a critical infrastructure asset. The pre-conditions for a Ministerial authorisation would serve to ensure a comprehensive appreciation for the incident, its impacts and the impacts of a direction. It would also ensure directions remain a last resort and do not impede any ongoing law

enforcement or regulatory action.

Summary of changes

This Part would achieve this by the introduction of two key changes to Part 3A of the SOCI Act, specifically:

- The phrase 'a cyber security incident' will be substituted with 'an incident' or 'an incident that has had, is having, or is likely to have, a relevant impact on one or more critical infrastructure assets' throughout Part 3A as appropriate.
 - o This amendment ensures Part 3A is available in circumstances beyond an initial response, for both cyber and non-cyber related incidents impacting critical infrastructure assets and cascading impacts to other critical infrastructure sector assets.
- Clarification of the pre-requisites and the sequence of steps required before Ministerial authorisation may be given.
 - o Amendments to section 35AB clarifies that an action direction requiring an entity to disclose personal information will require agreement from the Minister administering the *Privacy Act 1988*.

Ministerial authorisation for intervention requests would remain limited to cyber security incidents.

Part 3—Use and disclosure of protected information

Introductory comments

The amendments contained within this Part would implement Measure 7 of the Consultation Paper, introducing a revised harms based definition of 'protected information' and clarifying disclosure provisions.

The protected information provisions under the SOCI Act were designed to apply similar information sharing restrictions on private entities operating critical infrastructure to those found on public service employees. However, feedback from all levels of government and industry has demonstrated that the SOCI Act may in some instances unnecessarily limit the ability of Government, responsible entities and their employees to use or disclose information in the course of ordinary business, mitigate relevant risk effectively, and hobbling the response to high risk or time sensitive events.

The amendments to the definition of 'protected information' would clarify that a document or information is only protected information if the disclosure of that document or information could cause harm, or pose risk to the Australian public, the security of the asset, commercial interests, the socioeconomic stability, national security or defence of Australia.

Clarity for entities on what information is protected information and where disclosure may be authorised would provide entities confidence in their use and disclosure of protected information, limit disruption and undue burden of the regulatory framework on entities and facilitate broader security uplift by facilitating appropriate collaboration between industry and government.

Additionally, these amendments would clarify when critical infrastructure entities can disclose information. This includes through the new authorisation provisions for purposes relating to the continued operation of a critical infrastructure asset. Normal functions and duties for Department of Home Affairs continue to be authorised under the existing section 41 provision.

To ensure the provisions continue to operate in harmony with the Privacy Act, the use and disclosure provisions in Part 4 of the SOCI Act would continue to limit disclosure to circumstances where it is necessary and for an authorised purpose. Where protected information is personal information, disclosure would only be permitted where it is for a specified purpose and authorised by a specific provision under the SOCI Act, in accordance with a direction issued under the SOCI Act or otherwise authorised by law.

Summary of changes

This Part would introduce a new section 5A (which replaces the section 5 definition of protected information) and a number of new and revised provisions in Part 4 of the SOCI Act. In line with the findings of the Attorney General's Review of Secrecy Provisions, this secrecy regime would now require entities to consider, in determining whether information is 'protected information', the relative harm of disclosure. The amendments would:

- Introduce a new definition of 'protected information', which includes a harms-based assessment and a non-exhaustive list of 'relevant information';
- Clarify that entities may make a record of, use or disclose protected information where the purpose relates to the continued operation of an asset or to mitigate risks to that asset;
- Introduce a definition for 'authorised APS employee' and provisions which enable the Secretary to authorise APS employees to make a disclosure of protected information in the course of the duties, for example emailing the authorised documents to the entity;
- Introduce a definition for 'confidential commercial information' which outlines the type of information that is included within the definition of protected information and reassure the owners and operators of critical infrastructure that government agencies will treat commercially sensitive information in the same manner as security sensitive information; and
- Allow the Secretary to authorise disclosure of protected information to a Commonwealth, State and Territory Minister, agency head, or member of their staff, where the Minister or agency is responsible for emergency management, law enforcement or the regulation/oversight of the sector to which that critical infrastructure asset belongs.

These changes would make clear that the intended application of the use and disclosure provisions is to facilitate appropriate information protections and sharing to support security and resilience outcomes. Furthermore, the inclusion of 'relevant information' in section 5A would provide a non-exhaustive list of documents and categories of information they may consider when carrying out a "harms-based" assessment to determine whether information is protected information.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Part 4—Direction to vary critical infrastructure risk management program

Introductory comments

The amendments would implement Measure 8 of the Consultation Paper, dealing with enforcing critical infrastructure risk management obligations.

Specifically, the amendments would have the effect of enabling the regulator to issue directions to address serious deficiencies identified in a risk management program (RMP) held by a responsible entity as part of obligations under Part 2A. The ability for the regulator to issue such a direction would help ensure that RMP obligations achieve the intent of embedding preparation, prevention, and mitigation activities into the business-as-usual operations of critical infrastructure assets.

The Department intends for deficiencies to be assessed and directions issued in accordance with the CISC Compliance and Enforcement Strategy. Wherever possible, the CISC seeks to work in partnership with industry to ensure regulated entities understand and effectively manage their risks, reserving compliance levers as last resort measures.

Summary of changes

This Part would introduce a compliance 'review and remedy' power for the regulator to enforce RMP obligations on responsible entities of relevant critical infrastructure assets. This power would be effected by:

- new sections of the Act which empowers relevant officials to give the responsible entity a written direction to vary the entity's risk management program to address a serious deficiency;
- a new definitions for 'relevant official', which means the Secretary of Home Affairs or the relevant Commonwealth regulator (which is defined in section 5 of the SOCI Act and must be prescribed in the rules in relation to the relevant asset) and;
- a new definition of 'serious deficiency', which means a deficiency that poses a material risk to national security, the defence of Australia, or the social or economic stability of Australia or its people;
- a requirement for responsible entities to include the receipt of a direction and the remedy of the identified deficiency in their annual report; and
- a requirement to include details regarding the use of the direction within existing government reporting provisions.

The new sections would also provide for consultation requirements, time periods for response and compliance, and new civil penalties for non-compliance with a direction. A direction under this part would not be a legislative instrument within the meaning subsection 8(1) of the *Legislation Act 2003*.

Part 5—Security regulation for the telecommunications sector

Introductory comments

The amendments contained within this Part would implement Measure 9 of the Consultation Paper. Current security and related obligations under the Telecommunications Sector Security Reforms (which are amendments made by the *Telecommunications and Other Legislation Amendment Act 2017*) would be moved into the SOCI Act. These amendments have been consulted on in detail through the Australian Telecommunications Security Reference Group (ATSRG), a group comprising of Australian Government agencies, industry and industry peak bodies.

Critical incidents affecting telecommunications services have exposed a need to re-evaluate security regulation for telecommunications assets. Another incident affecting telecommunications services could pose severe economic and social consequences for Australians. Following an extensive consultation and co-design process with the ATSRG, the Department will progress reforms by uplifting aspects of security regulation from the Telecommunications Act to the SOCI Act.

The SOCI Act primarily regulates Australia's most critical assets through the entities who own, operate and influence them. The Telecommunications Act is primarily concerned with regulating carriers and carriage service providers (CSPs). One of the main aims of uplifting security regulation from the Telecommunications Act to the SOCI Act is to balance the impost of the regulatory framework on entities while ensuring national security outcomes. The Government must maintain its ability to oversee and intervene as required in Australia's telecommunications infrastructure. To achieve this, amendments to the SOCI Act intend to maintain a high-level capture of all carriers and CSPs in Australia; with the details on limiting the application of obligations in delegated legislation.

The amendments contained within this Part would achieve this by uplifting and aligning key security obligations from Part 14 of the Telecommunications Act into the SOCI Act, including a Ministerial direction power to manage circumstances where the use or supply of carriage services are prejudicial to security. Further, telecommunications security requirements under the SOCI Act would include requirements for the subset of critical telecommunication assets to:

- protect critical telecommunications assets as far as it is reasonably practicable to do so;
- notify the Home Affairs Secretary of security risks incurred by network changes of the critical telecommunications asset; and
- manage risks in line with a bespoke Telecommunications Security and Risk Management Program (TSRMP), the further details of which will be set out in subordinate legislation.
 - o The TSRMP Rules would be a legislative instrument authorised by the SOCI Act, and contain details on how entities can meet the positive security obligations outlined above. These Rules would embed the connection between the obligations to protect the asset, manage risk, and notify of changes to the asset.

The Telecommunications (Carrier License Conditions—Security Information) Declaration 2022 and the Telecommunications (Carriage Service Provider—Security Information) Determination 2022, which currently apply equivalent obligations for the Register of Critical Infrastructure Assets and Mandatory Cyber Incident Reporting would be repealed. These obligations will be switched on under the Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022, for a subset of critical telecommunications assets. All subordinate legislation changes would be progressed after passage of the Bill and would be subject to a formal 28-day consultation period.

Summary of changes

This Part would consolidate security requirements for critical telecommunications assets from Part 14 of the Telecommunications Act into the SOCI Act. The measures include:

- Preserving the capture of carriers and CSPs. This is intended to align the status quo under the Telecommunications Act with the SOCI Act's application to "assets" and the owners and operators of those assets.
- Integrating and aligning obligations from the Telecommunications Act with obligations under the SOCI Act and clarifying those obligations.
 - o A new Part creating enhanced obligations for critical telecommunications assets would be established in the SOCI Act.
 - o The 'security' obligation (from section 313(1A) of the Telecommunications Act) will be aligned with the SOCI Act by expanding it from its current limited focus on security risks (for example espionage and sabotage) to include all hazards. This will ensure alignment with the risk management program obligation under the SOCI Act.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

- o The notification obligation (from sections 314A & 314B of the Telecommunications Act) would be integrated and clarified.
- Transitioning the Ministerial direction power where use or supply of carriage services is prejudicial to security from the Telecommunications Act to the SOCI Act.
- Activating the Register of Critical Infrastructure Assets and Mandatory Cyber Incident Reporting for a subset of critical telecommunications assets through subordinate legislation under the SOCI Act. The amendment to the Rules would be progressed after passage of the Bill and would be subject to the mandatory 28-day consultation period.
- Introducing bespoke TSRMP Rules for a subset of critical telecommunications assets under the SOCI Act, which would provide further details on compliance with the risk management program obligation and provide further clarity on the notification obligation. The TSRMP Rules would be progressed after the passage of the Bill and would be subject to the mandatory 28-day consultation period.

Consequential amendments would be made to reflect the movement of provisions from the Telecommunications Act to the SOCI Act. This includes amendments to the Telecommunications Act, the *Telecommunications (Interception and Access) Act 1979* and the *Australian Security Intelligence Organisation Act 1979*. Additional consequential amendments may be required prior to finalisation of the Bill for introduction.

A placeholder has also been included for transitional and savings provisions. These will be finalised prior to introduction of the Bill. Broadly speaking, these provisions would ensure preservation of actions taken under the Telecommunications Act and continuity of obligations during the transitional period prior to subordinate legislation taking effect.

Part 6—Notification of declaration of system of national significance

Introductory comments

The amendments contained within this Part would remove direct interest holders from administrative obligations associated with SoNS.

The Minister for Home Affairs may declare a critical infrastructure asset to be a SoNS under Part 6A of the SOCI Act. Consultation must be undertaken with the responsible entity. Under paragraph 52B(3)(a) of the SOCI Act, following the making of a declaration, the Minister must notify each reporting entity for the asset within 30 days after making the declaration.

Tracking and reporting on all changes to joint interest arrangements is an unreasonably onerous responsibility for a responsible entity. This is particularly when direct interest holders are also required to report changes directly to the Secretary through the Register of Critical Infrastructure Assets obligation. Reporting obligations for direct interest holders come into effect at the time the asset becomes a critical infrastructure asset. As an asset must be a critical infrastructure asset prior to the asset being declared a SoNS, the declaration of an asset as a SoNS does not remove or alter existing reporting obligations for the relevant responsible entity. Responsible entities would not be inhibited from notifying direct interest holders or relevant entities themselves, where appropriate, in accordance with the protected information sharing provisions.

This would not remove the requirement for direct interest holders to report interest and control or to provide information for the Register of Critical Infrastructure Assets at the time that an asset becomes a critical infrastructure asset, or when they meet or exceed the interest and control provisions where the asset is already a critical infrastructure asset. As such there would be no reduction in Government visibility of foreign investment risk.

Additionally, the Secretary will still be required to consult the direct interest holders as the relevant entity where the Secretary intends to apply an 'enhanced cyber security obligation' to the relevant entity under Division 5 of Part 2C of the SOCI Act.

Summary of changes

This Part would remove a requirement for the Minister to notify direct interest holders of a declaration of an asset as a SoNS, and for responsible entities to advise the Secretary of all instances when direct interest holders change for a given asset. Two key items would effect the changes for this Part:

- The Minister would no longer be required to notify each reporting entity for the asset under s 52B(3)(a) of the SOCI Act, but would be required to notify the responsible entity for the asset within 30 days after declaring the asset to be a SoNS.
- Responsible entities for an asset that is a declared SoNS would only need to notify the Secretary if that entity ceases to be the responsible entity under s 52D. This would remove an existing requirement for a responsible entity to advise the Secretary of changes to direct interest holders.

These changes would protect the identity of SoNS and avoids the risk of incorrect or inappropriate information disclosures to or about entities other than the responsible entity by any concerned parties. Direct interest holders would still be required to report on changes through the Register of Critical Infrastructure Assets obligation in Part 2 of the SOCI Act.