

EXPOSURE DRAFT



Australian Government
Department of Home Affairs



CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Exposure Draft

December 2021

EXPOSURE DRAFT

EXPOSURE DRAFT

2019-2020-2021-2022

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

EXPOSURE DRAFT

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

No. , 2022

(Home Affairs)

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

EXPOSURE DRAFT

EXPOSURE DRAFT

1

Commencement information

Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. The whole of this Act	The day after this Act receives the Royal Assent.	

2

Note: This table relates only to the provisions of this Act as originally enacted.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

3

4

5

(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.

6

7

8

3 Schedules

9

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

10

11

12

2

Security Legislation Amendment (Critical Infrastructure Protection)
Bill 2022

No. , 2022

EXPOSURE DRAFT

1 **Schedule 1—Amendments**
2

3 *AusCheck Act 2007*

4 **1 Subsection 4(1)**

5 Insert:

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

8 **2 After paragraph 8(1)(b)**

9 Insert:

10 (ba) a critical infrastructure risk management program permits a
11 background check of an individual to be conducted under the
12 AusCheck scheme; or

13 *Security of Critical Infrastructure Act 2018*

14 **3 After paragraph 3(b)**

15 Insert:

- 16 (c) requiring responsible entities for critical infrastructure assets
17 to identify and manage risks relating to those assets; and
18 (d) imposing enhanced cyber security obligations on relevant
19 entities for systems of national significance in order to
20 improve their preparedness for, and ability to respond to,
21 cyber security incidents; and

22 **4 Section 4**

23 After paragraph (a) of the paragraph beginning “The framework
24 consists of the following:”, insert:

25 (b) requiring the responsible entity for one or more critical
26 infrastructure assets to have, and comply with, a critical
27 infrastructure risk management program;

EXPOSURE DRAFT

Schedule 1 Amendments

1 **5 Section 4**

2 After paragraph (c) of the paragraph beginning “The framework
3 consists of the following:”, insert:

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

6 **6 Section 4**

7 After the paragraph beginning “The Minister may privately declare”,
8 insert:

9 The Minister may privately declare a critical infrastructure asset to
10 be a system of national significance.

11 **7 Section 5 (paragraph (c) of the definition of *critical energy***
12 ***market operator asset*)**

13 After “market”, insert “or system”.

14 **8 Section 5**

15 Insert:

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

18 *custodial or depository service* has the same meaning as in the
19 *Corporations Act 2001*.

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

21 **9 Section 5 (paragraphs (a) and (b) of the definition of *data***
22 ***storage or processing service*)**

23 Repeal the paragraphs, substitute:

24 (a) a service that:

25 (i) enables end-users to store or back-up data; and

26 (ii) is provided on a commercial basis; or

27 (b) a data processing service that:

28 (i) involves the use of one or more computers; and

1 (ii) is provided on a commercial basis.

2 **10 Section 5**

3 Insert:

4 *designated officer* has the meaning given by section 30DQ.

5 *evaluation report* has the meaning given by section 30CS.

6 *external auditor* means a person authorised under section 30CT to
7 be an external auditor for the purposes of this Act.

8 **11 Section 5 (definition of *higher education and research***
9 ***sector*)**

10 Repeal the definition, substitute:

11 *higher education and research sector* means the sector of the
12 Australian economy that involves undertaking a program of
13 research that is:

14 (a) supported financially (in whole or in part) by the
15 Commonwealth; or

16 (b) critical to:

17 (i) a critical infrastructure sector (other than the higher
18 education and research sector); or

19 (ii) national security; or

20 (iii) the defence of Australia.

21 **12 Section 5**

22 Insert:

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

24 **13 Section 5 (at the end of the definition of *notification***
25 ***provision*)**

26 Add:

27 ; or (r) subsection 52B(3); or

28 (s) subsection 52D(4).

EXPOSURE DRAFT

Schedule 1 Amendments

1 **14 Section 5 (after paragraph (b) of the definition of *protected***
2 ***information*)**

3 Insert:

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

6 **15 Section 5 (after paragraph (bb) of the definition of**
7 ***protected information*)**

8 Insert:

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

12 (bd) is, or is included in, a report that is given under
13 section 30AG; or

14 **16 Section 5 (after paragraph (be) of the definition of**
15 ***protected information*)**

16 Insert:

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

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

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

23 **17 Section 5 (definition of *registrable superannuation entity*)**

24 Repeal the definition.

25 **18 Section 5**

26 Insert:

27 ***related company group*** means a group of 2 or more bodies
28 corporate, where each member of the group is related to each other
29 member of the group. For this purpose, the question whether a
30 body corporate is related to another body corporate is to be
31 determined in the same manner as that question is determined
32 under the *Corporations Act 2001*.

EXPOSURE DRAFT

Amendments **Schedule 1**

1 **19 Section 5**

2 Insert:

3 *RSE licensee* has the same meaning as in the *Superannuation*
4 *Industry (Supervision) Act 1993*.

5 **20 Section 5 (paragraph (a) of the definition of security)**

6 Omit “and 12N”, substitute “, 12N, 30AG, 30CB, 30CM, 30CR, 30CU
7 and 30CW”.

8 **21 Section 5 (paragraph (b) of the definition of security)**

9 Omit “and 12N”, substitute “, 12N, 30AG, 30CB, 30CM, 30CR, 30CU
10 and 30CW”.

11 **22 Section 5**

12 Insert:

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

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

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

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

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

22 *vulnerability assessment report* has the meaning given by
23 section 30DA.

24 **23 At the end of section 8G**

25 Add:

26 (3) Each of the following is a *relevant impact* of a cyber security
27 incident on a system of national significance:

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (a) the impact (whether direct or indirect) of the incident on the
2 availability of the system;
- 3 (b) the impact (whether direct or indirect) of the incident on the
4 integrity of the system;
- 5 (c) the impact (whether direct or indirect) of the incident on the
6 reliability of the system;
- 7 (d) the impact (whether direct or indirect) of the incident on the
8 confidentiality of:
- 9 (i) information about the system; or
10 (ii) if information is stored in the system—the information;
11 or
12 (iii) if the system is computer data—the computer data.

24 Paragraph 12F(1)(b)

13 Omit “wholly or primarily”.

25 Paragraph 12F(1)(b)

14 Omit “on a commercial basis”.

26 After paragraph 12F(1)(c)

15 Insert:

16 ; and (d) the asset is not a critical telecommunications asset.

27 Paragraph 12F(2)(b)

17 Omit “wholly or primarily”.

28 Subparagraph 12F(2)(b)(i)

18 Omit “on a commercial basis”.

29 After paragraph 12F(2)(c)

19 Insert:

20 ; and (d) the asset is not a critical telecommunications asset.

30 Paragraph 12J(1)(a)

21 Omit “a registrable superannuation entity”, substitute “an RSE
22 licensee”.

1 **31 Paragraph 12J(2)(a)**

2 Omit “registrable superannuation entities”, substitute “RSE licensees”.

3 **32 Paragraph 12J(2)(b)**

4 Omit “a registrable superannuation entity”, substitute “an RSE
5 licensee”.

6 **33 After paragraph 12KA(1)(b)**

7 Insert:

8 ; and (c) is an asset that, in accordance with subsection (3), is critical
9 to the administration of an Australian domain name system.

10 **34 At the end of section 12KA**

11 Add:

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

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

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

17 **35 Paragraph 12L(6)(a)**

18 Omit “registrable superannuation entity”, substitute “RSE licensee”.

19 **36 At the end of section 12L**

20 Add:

21 *System of national significance*

22 (25) If a critical infrastructure asset is a system of national significance,
23 the responsible entity for the system of national significance is the
24 responsible entity for the asset.

25 **37 After Part 2**

26 Insert:

EXPOSURE DRAFT

Schedule 1 Amendments

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

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

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

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

24 **30AB Application of this Part**

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

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

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

4 (3) The rules may provide that, if an asset becomes a critical
5 infrastructure asset, this Part does not apply to the asset during the
6 period:

7 (a) beginning when the asset became a critical infrastructure
8 asset; and

9 (b) ending at a time ascertained in accordance with the rules.

10 **30ABA Consultation—rules**

11 *Scope*

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

14 *Consultation*

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

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

17 (i) setting out the draft rules or amendments; and

18 (ii) inviting persons to make submissions to the Minister
19 about the draft rules or amendments within 28 days after
20 the notice is published; and

21 (b) give a copy of the notice to each First Minister; and

22 (c) consider any submissions received within the 28-day period
23 mentioned in paragraph (a).

24 **30AC Responsible entity must have a critical infrastructure risk 25 management program**

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

28 (a) adopt; and

29 (b) maintain;

EXPOSURE DRAFT

Schedule 1 Amendments

1 a critical infrastructure risk management program that applies to
2 the entity.

3 Civil penalty: 200 penalty units.

4 **30AD Compliance with critical infrastructure risk management** 5 **program**

6 If:

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

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

11 the entity must comply with:

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

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

15 Civil penalty: 200 penalty units.

16 **30AE Review of critical infrastructure risk management program**

17 If:

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

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

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

23 Civil penalty: 200 penalty units.

24 **30AF Update of critical infrastructure risk management program**

25 If:

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

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

1 the entity must take all reasonable steps to ensure that the program
2 is up to date.

3 Civil penalty: 200 penalty units.

4 **30AG Responsible entity must submit annual report**

5 *Scope*

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

- 8 (a) an entity was the responsible entity for one or more critical
9 infrastructure assets; and
10 (b) the entity had a critical infrastructure risk management
11 program that applied to the entity.

12 *Annual report*

13 (2) The entity must, within 90 days after the end of the financial year,
14 give:

- 15 (a) if there is a relevant Commonwealth regulator that has
16 functions relating to the security of those assets—the relevant
17 Commonwealth regulator; or

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

19 a report that:

20 (c) if the entity had the program at the end of the financial
21 year—includes whichever of the following statements is
22 applicable:

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

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

27 (d) if a hazard had a significant relevant impact on one or more
28 of those assets during the relevant period—includes a
29 statement that:

30 (i) identifies the hazard; and

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (ii) evaluates the effectiveness of the program in mitigating
2 the significant relevant impact of the hazard on the
3 assets concerned; and
4 (iii) if the program was varied during the financial year as a
5 result of the occurrence of the hazard—outlines the
6 variation; and
7 (e) is in the approved form; and
8 (f) if the entity has a board, council or other governing body—is
9 approved by the board, council or other governing body, as
10 the case requires.

11 Civil penalty: 150 penalty units.

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

15 **30AH Critical infrastructure risk management program**

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

EXPOSURE DRAFT

Amendments **Schedule 1**

- 1 (b) may relate to one or more specified critical infrastructure
2 assets.
- 3 Note: For specification by class, see subsection 13(3) of the *Legislation Act*
4 *2003*.
- 5 (3) Subsection (2) of this section does not, by implication, limit
6 subsection 33(3A) of the *Acts Interpretation Act 1901*.
- 7 (4) Rules made for the purposes of paragraph (1)(c) may require that a
8 critical infrastructure risk management program include one or
9 more provisions that permit a background check of an individual to
10 be conducted under the AusCheck scheme.
- 11 (5) Subsection (4) does not limit paragraph (1)(c).
- 12 (6) In specifying requirements in rules made for the purposes of
13 paragraph (1)(c), the Minister must have regard to the following
14 matters:
- 15 (a) any existing regulatory system of the Commonwealth, a State
16 or a Territory that imposes obligations on responsible
17 entities;
- 18 (b) the costs that are likely to be incurred by responsible entities
19 in complying with those rules;
- 20 (c) the reasonableness and proportionality of the requirements in
21 relation to the purpose referred to in paragraph (1)(b);
- 22 (d) such other matters (if any) as the Minister considers relevant.
- 23 (7) For the purposes of this section, in determining whether a risk is a
24 material risk, regard must be had to:
- 25 (a) the likelihood of the hazard occurring; and
26 (b) the relevant impact of the hazard on the asset if the hazard
27 were to occur.
- 28 (8) The rules may provide that a specified risk is taken to be a material
29 risk for the purposes of this section.
- 30 (9) The rules may provide that the taking of specified action in relation
31 to a critical infrastructure asset is taken to be action that minimises
32 or eliminates any material risk that the occurrence of a specified
33 hazard could have a relevant impact on the asset.

EXPOSURE DRAFT

EXPOSURE DRAFT

Schedule 1 Amendments

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

3 (10) The rules may provide that the taking of specified action in relation
4 to a specified critical infrastructure asset is taken to be action that
5 minimises or eliminates any material risk that the occurrence of a
6 specified hazard could have a relevant impact on the asset.

7 Note: For specification by class, see subsection 13(3) of the *Legislation Act*
8 2003.

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

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

14 (12) The rules may provide that the taking of specified action in relation
15 to a specified critical infrastructure asset is taken to be action that
16 mitigates the relevant impact of a specified hazard on the asset.

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

19 **30AJ Variation of critical infrastructure risk management program**

20 A critical infrastructure risk management program may be varied,
21 so long as the varied program is a critical infrastructure risk
22 management program.

23 **30AK Revocation of adoption of critical infrastructure risk 24 management program**

25 If an entity has adopted a critical infrastructure risk management
26 program that applies to the entity, this Part does not prevent the
27 entity from:

- 28 (a) revoking that adoption; and
29 (b) adopting another critical infrastructure risk management
30 program that applies to the entity.

1 **30AL Consultation—rules**

2 *Scope*

- 3 (1) This section applies to rules made for the purposes of
4 section 30AH.

5 *Consultation*

- 6 (2) Before making or amending the rules, the Minister must:
7 (a) cause to be published on the Department’s website a notice:
8 (i) setting out the draft rules or amendments; and
9 (ii) inviting persons to make submissions to the Minister
10 about the draft rules or amendments within 28 days after
11 the notice is published; and
12 (b) give a copy of the notice to each First Minister; and
13 (c) consider any submissions received within the 28-day period
14 mentioned in paragraph (a).
- 15 (3) Subsection (2) does not apply if:
16 (a) the Minister is satisfied that there is an imminent threat that a
17 hazard will have a significant relevant impact on a critical
18 infrastructure asset; or
19 (b) the Minister is satisfied that a hazard has had, or is having, a
20 significant relevant impact on a critical infrastructure asset.

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

22 **30AM Review of rules**

23 *Scope*

- 24 (1) This section applies if, because of subsection 30AL(3),
25 subsection 30AL(2) did not apply to the making of:
26 (a) rules; or
27 (b) amendments.

28 *Review of rules*

- 29 (2) The Secretary must:
-

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (a) if paragraph (1)(a) applies—review the operation,
2 effectiveness and implications of the rules; and
3 (b) if paragraph (1)(b) applies—review the operation,
4 effectiveness and implications of the amendments; and
5 (c) without limiting paragraph (a) or (b), consider whether any
6 amendments should be made; and
7 (d) give the Minister:
8 (i) a report of the review; and
9 (ii) a statement setting out the Secretary’s findings.
- 10 (3) For the purposes of the review, the Secretary must:
11 (a) cause to be published on the Department’s website a notice:
12 (i) setting out the rules or amendments concerned; and
13 (ii) inviting persons to make submissions to the Secretary
14 about the rules or amendments concerned within 28
15 days after the notice is published; and
16 (b) give a copy of the notice to each First Minister; and
17 (c) consider any submissions received within the 28-day period
18 mentioned in paragraph (a).
- 19 (4) The Secretary must complete the review within 60 days after the
20 commencement of the rules or amendments concerned.

Minister to table statement of findings

- 21
22 (5) The Minister must cause a copy of the statement of findings to be
23 tabled in each House of the Parliament within 15 sitting days of
24 that House after the Minister receives it.

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

Scope

- 27
28 (1) This section applies to rules made for the purposes of
29 section 30AH.

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (a) an entity (the *first entity*) is or was subject to a requirement
2 under section 30BC or 30BD; and
3 (b) another entity (the *contracted service provider*) is or was:
4 (i) a party to a contract with the first entity; and
5 (ii) responsible under the contract for the provision of
6 services to the first entity;
7 then:
8 (c) the contracted service provider is not liable to an action or
9 other proceeding for damages for or in relation to an act done
10 or omitted in good faith for the purposes of ensuring or
11 facilitating compliance with the requirement; and
12 (d) an officer, employee or agent of the contracted service
13 provider is not liable to an action or other proceeding for
14 damages for or in relation to an act done or omitted in good
15 faith for the purposes of ensuring or facilitating compliance
16 with the requirement.

39 After Part 2B

17 Insert:
18

19 Part 2C—Enhanced cyber security obligations

20 Division 1—Simplified outline of this Part

21 30CA Simplified outline of this Part

- 22 • This Part sets out enhanced cyber security obligations that
23 relate to systems of national significance.
- 24 • The responsible entity for a system of national significance
25 may be subject to statutory incident response planning
26 obligations.
- 27 • The responsible entity for a system of national significance
28 may be required to undertake a cyber security exercise.

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

- The responsible entity for a system of national significance may be required to undertake a vulnerability assessment.
- If a computer is a system of national significance, or is needed to operate a system of national significance, a relevant entity for the system may be required to:
 - (a) give ASD periodic reports of system information; or
 - (b) give ASD event-based reports of system information; or
 - (c) install software that transmits system information to ASD.

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

Division 2—Statutory incident response planning obligations

Subdivision A—Application of statutory incident response planning obligations

30CB Application of statutory incident response planning obligations—determination by the Secretary

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

EXPOSURE DRAFT

Schedule 1 Amendments

1 (b) if there is a relevant Commonwealth regulator that has
2 functions relating to the security of that system—the relevant
3 Commonwealth regulator.

4 (5) A determination under this section is not a legislative instrument.

5 **30CC Revocation of determination**

6 *Scope*

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

10 *Power to revoke determination*

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

13 *Application of the Acts Interpretation Act 1901*

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

18 **Subdivision B—Statutory incident response planning** 19 **obligations**

20 **30CD Responsible entity must have an incident response plan**

- 21 If:
22 (a) an entity is the responsible entity for a system of national
23 significance; and
24 (b) the statutory incident response planning obligations apply to
25 the entity in relation to:
26 (i) the system; and
27 (ii) cyber security incidents;
28 the entity must:

- 1 (c) adopt; and
- 2 (d) maintain;
- 3 an incident response plan that applies to the entity in relation to:
- 4 (e) the system; and
- 5 (f) cyber security incidents.

6 Civil penalty: 200 penalty units.

7 **30CE Compliance with incident response plan**

8 If:

- 9 (a) an entity is the responsible entity for a system of national
 - 10 significance; and
 - 11 (b) the entity has adopted an incident response plan that applies
 - 12 to the entity;
- 13 the entity must comply with:
- 14 (c) the incident response plan; or
 - 15 (d) if the plan has been varied on one or more occasions—the
 - 16 plan as varied.

17 Civil penalty: 200 penalty units.

18 **30CF Review of incident response plan**

19 If:

- 20 (a) an entity is the responsible entity for a system of national
 - 21 significance; and
 - 22 (b) the entity has adopted an incident response plan that applies
 - 23 to the entity;
- 24 the entity must review the plan on a regular basis.

25 Civil penalty: 200 penalty units.

26 **30CG Update of incident response plan**

27 If:

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

EXPOSURE DRAFT

Schedule 1 Amendments

1 (b) the entity has adopted an incident response plan that applies
2 to the entity;
3 the entity must take all reasonable steps to ensure that the plan is
4 up to date.

5 Civil penalty: 200 penalty units.

6 **30CH Copy of incident response plan must be given to the Secretary**

7 (1) If:

8 (a) an entity is the responsible entity for a system of national
9 significance; and

10 (b) the entity adopts an incident response plan that applies to the
11 entity;

12 the entity must:

13 (c) provide a copy of the incident response plan to the Secretary;
14 and

15 (d) do so as soon as practicable after the adoption.

16 Civil penalty: 200 penalty units.

17 (2) If:

18 (a) an entity is the responsible entity for a system of national
19 significance; and

20 (b) the entity varies an incident response plan that applies to the
21 entity;

22 the entity must:

23 (c) provide a copy of the varied incident response plan to the
24 Secretary; and

25 (d) do so as soon as practicable after the variation.

26 Civil penalty: 200 penalty units.

27 **30CJ Incident response plan**

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

29 (a) that applies to an entity that is the responsible entity for a
30 system of national significance; and

31 (b) that relates to the system; and

EXPOSURE DRAFT

Amendments **Schedule 1**

- 1 (c) that relates to cyber security incidents; and
2 (d) the purpose of which is to plan for responding to cyber
3 security incidents that could have a relevant impact on the
4 system; and
5 (e) that complies with such requirements (if any) as are specified
6 in the rules.

- 7 (2) Requirements specified under paragraph (1)(e):
8 (a) may be of general application; or
9 (b) may relate to one or more specified systems of national
10 significance; or
11 (c) may relate to one or more specified types of cyber security
12 incidents.

13 Note: For specification by class, see subsection 13(3) of the *Legislation Act*
14 *2003*.

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

17 **30CK Variation of incident response plan**

18 An incident response plan may be varied, so long as the varied plan
19 is an incident response plan.

20 **30CL Revocation of adoption of incident response plan**

21 If an entity has adopted an incident response plan that applies to
22 the entity, this Division does not prevent the entity from:
23 (a) revoking that adoption; and
24 (b) adopting another incident response plan that applies to the
25 entity.

26 **Division 3—Cyber security exercises**

27 **30CM Requirement to undertake cyber security exercise**

- 28 (1) The Secretary may, by written notice given to an entity that is the
29 responsible entity for a system of national significance, require the
30 entity to:

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (a) undertake a cyber security exercise in relation to:
2 (i) the system; and
3 (ii) all types of cyber security incidents; and
4 (b) do so within the period specified in the notice.
- 5 (2) The Secretary may, by written notice given to an entity that is the
6 responsible entity for a system of national significance, require the
7 entity to:
8 (a) undertake a cyber security exercise in relation to:
9 (i) the system; and
10 (ii) one or more specified types of cyber security incidents;
11 and
12 (b) do so within the period specified in the notice.
- 13 (3) The period specified in a notice under subsection (1) or (2) must
14 not be earlier than the end of the 30-day period that began when
15 the notice was given.
- 16 (4) A notice under subsection (1) or (2) may also require the entity to
17 do any or all of the following things:
18 (a) allow one or more specified designated officers to observe
19 the cyber security exercise;
20 (b) provide those designated officers with access to premises for
21 the purposes of observing the cyber security exercise;
22 (c) provide those designated officers with reasonable assistance
23 and facilities that are reasonably necessary to allow those
24 designated officers to observe the cyber security exercise;
25 (d) allow those designated officers to make such records as are
26 reasonably necessary for the purposes of monitoring
27 compliance with the notice;
28 (e) give those designated officers reasonable notice of the time
29 when the cyber security exercise will begin.
- 30 (5) Before giving a notice to an entity under subsection (1) or (2) in
31 relation to a system of national significance, the Secretary must
32 consult:
33 (a) the entity; and

- 1 (b) if there is a relevant Commonwealth regulator that has
2 functions relating to the security of that system—the relevant
3 Commonwealth regulator.

4 **30CN Cyber security exercise**

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

EXPOSURE DRAFT

Schedule 1 Amendments

1 (f) that complies with such requirements (if any) as are specified
2 in the rules.

3 (2) Requirements specified under paragraph (1)(f):

4 (a) may be of general application; or

5 (b) may relate to one or more specified systems of national
6 significance; or

7 (c) may relate to one or more specified types of cyber security
8 incidents.

9 Note: For specification by class, see subsection 13(3) of the *Legislation Act*
10 *2003*.

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

13 **30CP Compliance with requirement to undertake cyber security** 14 **exercise**

15 An entity must comply with a notice given to the entity under
16 section 30CM.

17 Civil penalty: 200 penalty units.

18 **30CQ Internal evaluation report**

19 (1) If an entity undertakes a cyber security exercise under
20 section 30CM, the entity must:

21 (a) do both of the following:

22 (i) prepare an evaluation report relating to the cyber
23 security exercise;

24 (ii) give a copy of the report to the Secretary; and

25 (b) do so:

26 (i) within 30 days after the completion of the exercise; or

27 (ii) if the Secretary allows a longer period—within that
28 longer period.

29 Civil penalty: 200 penalty units.

- 1 (2) An evaluation report prepared by an entity under subsection (1) is
2 not admissible in evidence against the entity in civil proceedings
3 relating to a contravention of a civil penalty provision of this Act
4 (other than subsection (1) of this section or subsection 30CR(6)).

5 **30CR External evaluation report**

6 *Scope*

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

18 *Requirement*

- 19 (2) The Secretary may, by written notice given to the entity, require
20 the entity to:
21 (a) appoint an external auditor; and
22 (b) arrange for the external auditor to prepare an evaluation
23 report (the ***new evaluation report***) relating to the exercise;
24 and
25 (c) arrange for the external auditor to give the new evaluation
26 report to the entity; and
27 (d) give the Secretary a copy of the new evaluation report within:
28 (i) the period specified in the notice; or
29 (ii) if the Secretary allows a longer period—that longer
30 period.
31 (3) The notice must specify:
32 (a) the matters to be covered by the new evaluation report; and

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (b) the form of the new evaluation report and the kinds of details
2 it is to contain.

3 *Consultation*

- 4 (4) Before giving a notice to an entity under this section in connection
5 with a cyber security exercise that relates to a system of national
6 significance, the Secretary must consult:
7 (a) the entity; and
8 (b) if there is a relevant Commonwealth regulator that has
9 functions relating to the security of that system—the relevant
10 Commonwealth regulator.

11 *Eligibility for appointment as an external auditor*

- 12 (5) An individual is not eligible to be appointed as an external auditor
13 by the entity if the individual is an officer, employee or agent of
14 the entity.

15 *Compliance*

- 16 (6) An entity must comply with a requirement under subsection (2).
17 Civil penalty: 200 penalty units.

18 *Immunity*

- 19 (7) The new evaluation report is not admissible in evidence against the
20 entity in civil proceedings relating to a contravention of a civil
21 penalty provision of this Act (other than subsection (6)).

22 **30CS Meaning of *evaluation report***

23 An *evaluation report*, in relation to a cyber security exercise that
24 was undertaken in relation to a system of national significance, is a
25 written report:

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

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

20 **30CT External auditors**

- 21 (1) The Secretary may, by writing, authorise a specified individual to
22 be an external auditor for the purposes of this Act.
23 Note: For specification by class, see subsection 33(3AB) of the *Acts*
24 *Interpretation Act 1901*.
25 (2) An authorisation under subsection (1) is not a legislative
26 instrument.

27 **Division 4—Vulnerability assessments**

28 **30CU Requirement to undertake vulnerability assessment**

- 29 (1) The Secretary may, by written notice given to an entity that is the
30 responsible entity for a system of national significance, require the
31 entity to:

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (a) undertake, or cause to be undertaken, a vulnerability
2 assessment in relation to:
3 (i) the system; and
4 (ii) all types of cyber security incidents; and
5 (b) do so within the period specified in the notice.
- 6 (2) The Secretary may, by written notice given to an entity that is the
7 responsible entity for a system of national significance, require the
8 entity to:
9 (a) undertake, or cause to be undertaken, a vulnerability
10 assessment in relation to:
11 (i) the system; and
12 (ii) one or more specified types of cyber security incidents;
13 and
14 (b) do so within the period specified in the notice.
- 15 (3) Before giving a notice to an entity under subsection (1) or (2) in
16 relation to the system of national significance, the Secretary must
17 consult:
18 (a) the entity; and
19 (b) if there is a relevant Commonwealth regulator that has
20 functions relating to the security of that system—the relevant
21 Commonwealth regulator.

22 **30CV Compliance with requirement to undertake a vulnerability** 23 **assessment**

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

26 Civil penalty: 200 penalty units.

27 **30CW Designated officers may undertake a vulnerability assessment**

28 *Scope*

- 29 (1) This section applies if:
30 (a) an entity is the responsible entity for a system of national
31 significance; and
-

EXPOSURE DRAFT

Amendments **Schedule 1**

- 1 (b) either:
2 (i) the Secretary has reasonable grounds to believe that if
3 the entity were to be given a notice under
4 subsection 30CU(1) or (2), the entity would not be
5 capable of complying with the notice; or
6 (ii) the entity has not complied with a notice given to the
7 entity under subsection 30CU(1) or (2).

8 *Request*

- 9 (2) The Secretary may give a designated officer a written request to:
10 (a) undertake a vulnerability assessment in relation to:
11 (i) the system; and
12 (ii) all types of cyber security incidents; and
13 (b) do so within the period specified in the request.
- 14 (3) The Secretary may give a designated officer a written request to:
15 (a) undertake a vulnerability assessment in relation to:
16 (i) the system; and
17 (ii) one or more specified types of cyber security incidents;
18 and
19 (b) do so within the period specified in the request.
- 20 (4) Before giving a request under subsection (2) or (3) in relation to
21 the system of national significance, the Secretary must consult:
22 (a) the entity; and
23 (b) if there is a relevant Commonwealth regulator that has
24 functions relating to the security of that system—the relevant
25 Commonwealth regulator.

26 *Requirement*

- 27 (5) If a request under subsection (2) or (3) is given to a designated
28 officer, the Secretary may, by written notice given to the entity,
29 require the entity to do any or all of the following things:
30 (a) provide the designated officer with access to premises for the
31 purposes of undertaking the vulnerability assessment;
32 (b) provide the designated officer with access to computers for
33 the purposes of undertaking the vulnerability assessment;
-

EXPOSURE DRAFT

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (c) provide the designated officer with reasonable assistance and
2 facilities that are reasonably necessary to allow the
3 designated officer to undertake the vulnerability assessment.

4 *Notification of request*

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

7 **30CX Compliance with requirement to provide reasonable**
8 **assistance etc.**

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

11 Civil penalty: 200 penalty units.

12 **30CY Vulnerability assessment**

- 13 (1) A *vulnerability assessment* is an assessment:
14 (a) that relates to a system of national significance; and
15 (b) that either:
16 (i) relates to all types of cyber security incidents; or
17 (ii) relates to one or more specified types of cyber security
18 incidents; and
19 (c) if the assessment relates to all types of cyber security
20 incidents—the purpose of which is to test the vulnerability of
21 the system to all types of cyber security incidents; and
22 (d) if the assessment relates to one or more specified types of
23 cyber security incidents—the purpose of which is to test the
24 vulnerability of the system to those types of cyber security
25 incidents; and
26 (e) that complies with such requirements (if any) as are specified
27 in the rules.
- 28 (2) Requirements specified under paragraph (1)(e):
29 (a) may be of general application; or
30 (b) may relate to one or more specified systems of national
31 significance; or

1 (c) may relate to one or more specified types of cyber security
2 incidents.

3 Note: For specification by class, see subsection 13(3) of the *Legislation Act*
4 *2003*.

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

7 **30CZ Vulnerability assessment report**

8 (1) If an entity undertakes, or causes to be undertaken, a vulnerability
9 assessment under section 30CU, the entity must:

10 (a) do both of the following:

11 (i) prepare, or cause to be prepared, a vulnerability
12 assessment report relating to the assessment;

13 (ii) give a copy of the report to the Secretary; and

14 (b) do so:

15 (i) within 30 days after the completion of the assessment;
16 or

17 (ii) if the Secretary allows a longer period—within that
18 longer period.

19 Civil penalty: 200 penalty units.

20 (2) If a designated officer undertakes a vulnerability assessment in
21 accordance with a request given to the designated officer under
22 section 30CW, the designated officer must:

23 (a) do both of the following:

24 (i) prepare a vulnerability assessment report relating to the
25 assessment;

26 (ii) give a copy of the report to the Secretary; and

27 (b) do so:

28 (i) within 30 days after the completion of the assessment;
29 or

30 (ii) if the Secretary allows a longer period—within that
31 longer period.

32 (3) If an entity prepares, or causes to be prepared, a report under
33 subsection (1), the report is not admissible in evidence against the

EXPOSURE DRAFT

Amendments **Schedule 1**

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

6 *Requirement*

- 7 (2) The Secretary may, by written notice given to the entity, require
8 the entity to:
9 (a) prepare periodic reports that:
10 (i) consist of any such information; and
11 (ii) relate to such regular intervals as are specified in the
12 notice; and
13 (b) prepare those periodic reports:
14 (i) in the manner and form specified in the notice; and
15 (ii) in accordance with the information technology
16 requirements specified in the notice; and
17 (c) give each of those periodic reports to ASD within the period
18 ascertained in accordance with the notice in relation to the
19 periodic report concerned.
- 20 (3) A notice under subsection (2) is to be known as a ***system***
21 ***information periodic reporting notice***.
- 22 (4) In deciding whether to give a system information periodic
23 reporting notice to the entity, the Secretary must have regard to:
24 (a) the costs that are likely to be incurred by the entity in
25 complying with the notice; and
26 (b) such other matters (if any) as the Secretary considers
27 relevant.

28 *Matters to be set out in notice*

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

EXPOSURE DRAFT

EXPOSURE DRAFT

Schedule 1 Amendments

1

Other powers not limited

2

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

3

4

30DC Secretary may require event-based reporting of system information

5

6

Scope

7

- (1) This section applies if:

8

- (a) a computer:

9

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

10

or

11

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

12

- (b) the Secretary believes on reasonable grounds that, each time

13

a particular kind of event occurs, a relevant entity for the

14

system of national significance will be technically capable of

15

preparing a report consisting of information that:

16

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

17

- (ii) may assist with determining whether a power under this

18

Act should be exercised in relation to the system of

19

national significance; and

20

- (iii) is not personal information (within the meaning of the

21

Privacy Act 1988).

22

Requirement

23

- (2) The Secretary may, by written notice given to the entity, require the entity to do the following things each time an event of that kind occurs:

24

25

- (a) prepare a report that consists of any such information;

26

- (b) prepare that report:

27

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

28

- (ii) in accordance with the information technology

29

requirements specified in the notice;

30

- (c) give that report to ASD as soon as practicable after the event

31

32

occurs.

1 (3) A notice under subsection (2) is to be known as a *system*
2 *information event-based reporting notice*.

3 (4) In deciding whether to give a system information event-based
4 reporting notice to the entity, the Secretary must have regard to:
5 (a) the costs that are likely to be incurred by the entity in
6 complying with the notice; and
7 (b) such other matters (if any) as the Secretary considers
8 relevant.

9 *Matters to be set out in notice*

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

12 *Other powers not limited*

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

15 **30DD Consultation**

16 Before giving:

- 17 (a) a system information periodic reporting notice; or
18 (b) a system information event-based reporting notice;
19 to a relevant entity for a system of national significance, the
20 Secretary must consult:
21 (c) the relevant entity; and
22 (d) if the relevant entity is not the responsible entity for the
23 system of national significance—the responsible entity for
24 the system of national significance.

25 **30DE Duration of system information periodic reporting notice or** 26 **system information event-based reporting notice**

- 27 (1) A system information periodic reporting notice or a system
28 information event-based reporting notice:
29 (a) comes into force:
30 (i) when it is given; or

EXPOSURE DRAFT

Schedule 1 Amendments

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

21 **30DF Compliance with system information periodic reporting notice** 22 **or system information event-based reporting notice**

23 An entity must comply with:

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

27 Civil penalty: 200 penalty units.

28 **30DG Self-incrimination etc.**

- 29 (1) An entity is not excused from giving a report under section 30DB
30 or 30DC on the ground that the report might tend to incriminate the
31 entity.

- 1 (2) If, at general law, an individual would otherwise be able to claim
2 the privilege against self-exposure to a penalty (other than a
3 penalty for an offence) in relation to giving a report under
4 section 30DB or 30DC, the individual is not excused from giving a
5 report under that section on that ground.

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

8 **30DH Admissibility of report etc.**

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

- 10 (a) the report; or
11 (b) giving the report;
12 is not admissible in evidence against an entity:
13 (c) in criminal proceedings other than proceedings for an offence
14 against section 137.2 of the *Criminal Code* that relates to this
15 Act; or
16 (d) in civil proceedings other than proceedings for recovery of a
17 penalty in relation to a contravention of section 30DF.

18 **Subdivision B—System information software**

19 **30DJ Secretary may require installation of system information** 20 **software**

21 *Scope*

- 22 (1) This section applies if:
23 (a) a computer:
24 (i) is needed to operate a system of national significance;
25 or
26 (ii) is a system of national significance; and
27 (b) the Secretary believes on reasonable grounds that a relevant
28 entity for the system of national significance would not be
29 technically capable of preparing reports under section 30DB
30 or 30DC consisting of information that:
31 (i) relates to the operation of the computer; and

EXPOSURE DRAFT

Schedule 1 Amendments

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

6 *Requirement*

- 7 (2) The Secretary may, by written notice given to the entity, require
8 the entity to:
9 (a) both:
10 (i) install a specified computer program on the computer;
11 and
12 (ii) do so within the period specified in the notice; and
13 (b) maintain the computer program installed in accordance with
14 paragraph (a); and
15 (c) take all reasonable steps to ensure that the computer is
16 continuously supplied with an internet carriage service that
17 enables the computer program to function.
- 18 (3) A notice under subsection (2) is to be known as a ***system***
19 ***information software notice***.
- 20 (4) In deciding whether to give a system information software notice
21 to the entity, the Secretary must have regard to:
22 (a) the costs that are likely to be incurred by the entity in
23 complying with the notice; and
24 (b) such other matters (if any) as the Secretary considers
25 relevant.
- 26 (5) A computer program may only be specified in a system
27 information software notice if the purpose of the computer
28 program is to:
29 (a) collect and record information that:
30 (i) relates to the operation of the computer; and
31 (ii) may assist with determining whether a power under this
32 Act should be exercised in relation to the system of
33 national significance; and

- 1 (iii) is not personal information (within the meaning of the
2 *Privacy Act 1988*); and
3 (b) cause the information to be transmitted electronically to
4 ASD.

5 *Matters to be set out in notice*

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

8 *Other powers not limited*

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

11 **30DK Consultation**

12 Before giving a system information software notice to a relevant
13 entity for a system of national significance, the Secretary must
14 consult:

- 15 (a) the relevant entity; and
16 (b) if the relevant entity is not the responsible entity for the
17 system of national significance—the responsible entity for
18 the system of national significance.

19 **30DL Duration of system information software notice**

- 20 (1) A system information software notice:
21 (a) comes into force:
22 (i) when it is given; or
23 (ii) if a later time is specified in the notice—at that later
24 time; and
25 (b) remains in force for the period specified in the notice.
- 26 (2) The period specified in the notice must not be longer than 12
27 months.
- 28 (3) If a system information software notice (the *original notice*) is in
29 force, this Act does not prevent the Secretary from giving a fresh
30 system information software notice that:

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (a) is in the same, or substantially the same, terms as the original
2 notice; and
3 (b) comes into force immediately after the expiry of the original
4 notice.

5 **30DM Compliance with system information software notice**

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

8 Civil penalty: 200 penalty units.

9 **30DN Self-incrimination etc.**

- 10 (1) An entity is not excused from complying with a system
11 information software notice on the ground that complying with the
12 notice might tend to incriminate the entity.
- 13 (2) If, at general law, an individual would otherwise be able to claim
14 the privilege against self-exposure to a penalty (other than a
15 penalty for an offence) in relation to complying with a system
16 information software notice, the individual is not excused from
17 complying with the notice on that ground.

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

20 **30DP Admissibility of information etc.**

21 If:

- 22 (a) a computer program is installed in compliance with a system
23 information software notice; and
24 (b) information is transmitted to ASD as a result of the operation
25 of the computer program;
26 the information is not admissible in evidence against an entity:
27 (c) in criminal proceedings; or
28 (d) in civil proceedings other than proceedings for recovery of a
29 penalty in relation to a contravention of section 30DM.

1 **Division 6—Designated officers**

2 **30DQ Designated officer**

- 3 (1) A *designated officer* is an individual appointed by the Secretary, in
4 writing, to be a designated officer for the purposes of this Act.
- 5 (2) The Secretary must not appoint an individual under subsection (1)
6 unless:
7 (a) the individual is a Departmental employee; or
8 (b) both:
9 (i) the individual is a staff member of ASD; and
10 (ii) the Director-General of ASD has agreed to the
11 appointment.
- 12 (3) The Secretary may, in writing, declare that each Departmental
13 employee included in a specified class of Departmental employees
14 is a designated officer.
- 15 (4) The Secretary may, in writing, declare that each staff member of
16 ASD included in a specified class of staff members of ASD is a
17 designated officer.
- 18 (5) The Secretary must not make a declaration under subsection (4)
19 unless the Director-General of ASD has agreed to the declaration.
- 20 (6) For the purposes of this section, *Departmental employee* means an
21 APS employee in the Department.
- 22 (7) For the purposes of this section, *staff member of ASD* has the
23 same meaning as in the *Intelligence Services Act 2001*.
- 24 (8) A declaration under this section is not a legislative instrument.

25 **40 After section 35**

26 Insert:

EXPOSURE DRAFT

Schedule 1 Amendments

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

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

7 **41 At the end of subsection 35AAB**

8 Add:

9 (3) If:

- 10 (a) an entity is or was subject to a direction under
11 subsection 32(2); and
12 (b) the entity is or was a member of a related company group;
13 then:
14 (c) another member of the related company group is not liable to
15 an action or other proceeding for damages for or in relation to
16 an act done or omitted in good faith for the purposes of
17 ensuring or facilitating compliance with the direction; and
18 (d) an officer, employee or agent of another member of the
19 related company group is not liable to an action or other
20 proceeding for damages for or in relation to an act done or
21 omitted in good faith for the purposes of ensuring or
22 facilitating compliance with the direction.

23 (4) If:

- 24 (a) an entity (the *first entity*) is or was subject to a direction
25 under subsection 32(2); and
26 (b) another entity (the *contracted service provider*) is or was:
27 (i) a party to a contract with the first entity; and
28 (ii) responsible under the contract for the provision of
29 services to the first entity;
30 then:
31 (c) the contracted service provider is not liable to an action or
32 other proceeding for damages for or in relation to an act done
33 or omitted in good faith for the purposes of ensuring or
34 facilitating compliance with the direction; and

- 1 (d) an officer, employee or agent of the contracted service
2 provider is not liable to an action or other proceeding for
3 damages for or in relation to an act done or omitted in good
4 faith for the purposes of ensuring or facilitating compliance
5 with the direction.

6 **42 After section 35AT**

7 Insert:

8 **35AU Directions prevail over inconsistent critical infrastructure risk**
9 **management programs**

10 If a critical infrastructure risk management program is applicable
11 to an entity, the program has no effect to the extent to which it is
12 inconsistent with a direction given to the entity under
13 section 35AQ.

14 **43 At the end of subsection 35AW**

15 Add:

16 (3) If:

- 17 (a) an entity is or was subject to a direction given under
18 section 35AQ; and
19 (b) the entity is or was a member of a related company group;

20 then:

- 21 (c) another member of the related company group is not liable to
22 an action or other proceeding for damages for or in relation to
23 an act done or omitted in good faith for the purposes of
24 ensuring or facilitating compliance with the direction; and
25 (d) an officer, employee or agent of another member of the
26 related company group is not liable to an action or other
27 proceeding for damages for or in relation to an act done or
28 omitted in good faith for the purposes of ensuring or
29 facilitating compliance with the direction.

30 (4) If:

- 31 (a) an entity (the *first entity*) is or was subject to a direction
32 given under section 35AQ; and

EXPOSURE DRAFT

Schedule 1 Amendments

- 1 (b) another entity (the *contracted service provider*) is or was:
2 (i) a party to a contract with the first entity; and
3 (ii) responsible under the contract for the provision of
4 services to the first entity;
5 then:
6 (c) the contracted service provider is not liable to an action or
7 other proceeding for damages for or in relation to an act done
8 or omitted in good faith for the purposes of ensuring or
9 facilitating compliance with the direction; and
10 (d) an officer, employee or agent of the contracted service
11 provider is not liable to an action or other proceeding for
12 damages for or in relation to an act done or omitted in good
13 faith for the purposes of ensuring or facilitating compliance
14 with the direction.

44 At the end of subsection 35BB

- 15 Add:
16
17 (6) If:
18 (a) an entity is or was subject to a requirement under
19 subsection (1); and
20 (b) the entity is or was a member of a related company group;
21 then:
22 (c) another member of the related company group is not liable to
23 an action or other proceeding for damages for or in relation to
24 an act done or omitted in good faith for the purposes of
25 ensuring or facilitating compliance with the requirement; and
26 (d) an officer, employee or agent of another member of the
27 related company group is not liable to an action or other
28 proceeding for damages for or in relation to an act done or
29 omitted in good faith for the purposes of ensuring or
30 facilitating compliance with the requirement.
31 (7) If:
32 (a) an entity (the *first entity*) is or was subject to a requirement
33 under subsection (1); and
34 (b) another entity (the *contracted service provider*) is or was:
35 (i) a party to a contract with the first entity; and
-

1 (ii) responsible under the contract for the provision of
2 services to the first entity;

3 then:

4 (c) the contracted service provider is not liable to an action or
5 other proceeding for damages for or in relation to an act done
6 or omitted in good faith for the purposes of ensuring or
7 facilitating compliance with the requirement; and

8 (d) an officer, employee or agent of the contracted service
9 provider is not liable to an action or other proceeding for
10 damages for or in relation to an act done or omitted in good
11 faith for the purposes of ensuring or facilitating compliance
12 with the requirement.

13 **45 After section 43D**

14 Insert:

15 **43E Authorised disclosure of protected information by the entity to** 16 **whom the information relates**

17 (1) An entity may disclose protected information if:

18 (a) the entity is the entity to whom the protected information
19 relates; and

20 (b) the entity discloses the protected information to:

21 (i) a Minister of the Commonwealth who has responsibility
22 for the regulation or oversight of the relevant critical
23 infrastructure sector to which the protected information
24 relates;

25 (ii) a Minister of a State, the Australian Capital Territory, or
26 the Northern Territory, who has responsibility for the
27 regulation or oversight of the relevant critical
28 infrastructure sector to which the protected information
29 relates;

30 (iii) a person employed as a member of staff of a Minister
31 mentioned in subparagraph (i) or (ii);

32 (iv) the head of an agency (including a Department)
33 administered by a Minister mentioned in
34 subparagraph (i) or (ii), or an officer or employee of that
35 agency; and

EXPOSURE DRAFT

Schedule 1 Amendments

1 (c) the disclosure to the person mentioned in paragraph (b) is for
2 the purposes of enabling or assisting the person to exercise
3 the person's powers or perform the person's functions or
4 duties.

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

7 (2) An entity may disclose protected information if:

8 (a) the entity is the entity to whom the protected information
9 relates; and

10 (b) the protected information is covered by:

11 (i) any of paragraphs (b) to (bl) of the definition of
12 *protected information* in section 5; or

13 (ii) paragraph (c) of that definition so far as that definition
14 relates to any of paragraphs (b) to (bl) of that definition;
15 and

16 (iii) the Secretary has consented, in writing, to the
17 disclosure; and

18 (iv) if the Secretary's consent is subject to one or more
19 conditions—those conditions are satisfied.

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

22 (3) An entity may disclose protected information if:

23 (a) the entity is the entity to whom the protected information
24 relates; and

25 (b) the protected information is not covered by:

26 (i) any of paragraphs (b) to (bl) of the definition of
27 *protected information* in section 5; or

28 (ii) paragraph (c) of that definition so far as that definition
29 relates to any of paragraphs (b) to (bl) of that definition.

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

32 **46 Subsection 46(2)**

33 After "critical infrastructure asset", insert "or of the fact that an asset is
34 declared under section 52B to be a system of national significance".

1 **47 Paragraph 46(4)(b)**

2 Repeal the paragraph.

3 **48 After paragraph 51(2A)(a)**

4 Insert:

5 (b) determine that Part 2A applies to the asset;

6 **49 After Part 6**

7 Insert:

8 **Part 6A—Declaration of systems of national**
9 **significance by the Minister**

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

11 **52A Simplified outline of this Part**

12 The Minister may privately declare a critical infrastructure asset to
13 be a system of national significance.

14 The Minister must notify each reporting entity for an asset that is a
15 declared system of national significance.

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

20 Note: It is an offence to disclose that an asset has been declared a system of
21 national significance (see section 45).

EXPOSURE DRAFT

Schedule 1 Amendments

1 **Division 2—Declaration of systems of national significance**
2 **by the Minister**

3 **52B Declaration of systems of national significance by the Minister**

- 4 (1) The Minister may, in writing, declare a particular asset to be a
5 system of national significance if:
6 (a) the asset is a critical infrastructure asset; and
7 (b) the Minister is satisfied that the asset is of national
8 significance.
- 9 (2) In determining whether an asset is of national significance for the
10 purposes of subsection (1), the Minister must have regard to:
11 (a) the consequences that would arise for:
12 (i) the social or economic stability of Australia or its
13 people; or
14 (ii) the defence of Australia; or
15 (iii) national security;
16 if a hazard were to occur that had a significant relevant
17 impact on the asset; and
18 (b) if the Minister is aware of one or more interdependencies
19 between the asset and one or more other critical infrastructure
20 assets—the nature and extent of those interdependencies; and
21 (c) such other matters (if any) as the Minister considers relevant.
- 22 (3) The Minister must notify the following of the declaration, in
23 writing, within 30 days after making the declaration in relation to
24 an asset:
25 (a) each reporting entity for the asset;
26 (b) if the asset is a tangible asset located (wholly or partly) in a
27 State, the Australian Capital Territory or the Northern
28 Territory—the First Minister of the State, the Australian
29 Capital Territory or the Northern Territory, as the case
30 requires.
- 31 (4) A declaration under subsection (1) is not a legislative instrument.

- 1 (5) To avoid doubt, an asset may be the subject of a declaration under
2 subsection (1) even if the asset is not a system.

3 **52C Consultation—declaration**

- 4 (1) Before making a declaration under section 52B in relation to an
5 asset, the Minister must give the responsible entity for the asset a
6 notice:
7 (a) setting out the proposed declaration; and
8 (b) inviting the entity to make submissions to the Minister about
9 the proposed declaration within:
10 (i) 28 days after the notice is given; or
11 (ii) if a shorter period is specified in the notice—that shorter
12 period.
- 13 (2) The Minister must consider any submissions received within:
14 (a) the 28-day period mentioned in subparagraph (1)(b)(i); or
15 (b) if a shorter period is specified in the notice—that shorter
16 period.
- 17 (3) The Minister must not specify a shorter period in the notice unless
18 the Minister is satisfied that the shorter period is necessary due to
19 urgent circumstances.
- 20 (4) The notice must set out the reasons for making the declaration,
21 unless the Minister is satisfied that doing so would be prejudicial to
22 security.

23 **52D Notification of change to reporting entities for asset**

24 *Scope*

- 25 (1) This section applies if a reporting entity (the *first entity*) for an
26 asset declared under subsection 52B(1) to be a system of national
27 significance:
28 (a) ceases to be a reporting entity for the asset; or
29 (b) becomes aware of another reporting entity for the asset
30 (whether or not as a result of the first entity ceasing to be a
31 reporting entity).

EXPOSURE DRAFT

Schedule 1 Amendments

1

Notification

2

- (2) The first entity must, within 30 days, notify the Secretary of the following:

3

4

(a) the fact in paragraph (1)(a) or (b) (as the case requires);

5

(b) if another entity is a reporting entity for the asset—the name of each other entity and the address of each other entity’s head office or principal place of business (to the extent known by the first entity).

6

7

8

9

Civil penalty: 150 penalty units.

10

- (3) The first entity must use the entity’s best endeavours to determine the name and relevant address of any other entity for the purposes of paragraph (2)(b).

11

12

13

- (4) If the Secretary is notified of another entity under paragraph (2)(b), the Secretary must notify the other entity of the declaration under subsection 52B(1), in writing, within 30 days after being notified under that paragraph.

14

15

16

52E Review of declaration

17

18

Scope

19

- (1) This section applies if an asset is declared under subsection 52B(1) to be a system of national significance.

20

21

Request

22

- (2) The responsible entity for the asset may, by written notice given to the Secretary, request the Secretary to review whether the asset is of national significance.

23

24

25

Requirement

26

- (3) The Secretary must, within 60 days after the request is given:

27

(a) review whether the asset is of national significance; and

28

(b) give the Minister:

29

(i) a report of the review; and

- 1 (ii) a statement setting out the Secretary’s findings.
- 2 (4) The review must be undertaken in consultation with the
3 responsible entity for the asset.
- 4 (5) In reviewing whether the asset is of national significance, the
5 Secretary must have regard to:
- 6 (a) the consequences that would arise for:
- 7 (i) the social or economic stability of Australia or its
8 people; or
- 9 (ii) the defence of Australia; or
- 10 (iii) national security;
- 11 if a hazard were to occur that had a significant relevant
12 impact on the asset; and
- 13 (b) if the Secretary is aware of one or more interdependencies
14 between the asset and one or more other critical infrastructure
15 assets—the nature and extent of those interdependencies; and
- 16 (c) such other matters (if any) as the Secretary considers
17 relevant.

18 *Limit*

- 19 (6) The responsible entity for the asset must not make more than one
20 request under subsection (2) in relation to the asset during a
21 12-month period.

22 **52F Revocation of determination**

23 *Scope*

- 24 (1) This section applies if:
- 25 (a) a declaration under subsection 52B(1) is in force in relation
26 to an asset; and
- 27 (b) the Minister is no longer satisfied that the asset is of national
28 significance.

29 *Duty to revoke declaration*

- 30 (2) The Minister must, in writing, revoke the declaration.

