Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Exposure Draft

December 2021

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

Contents

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

The Parliament of Australia enacts:

1 Short title

This Act is the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*.

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.

EXPOSURE DRAFT

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.	

Note: This table relates only to the provisions of this Act as originally enacted.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Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.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—Amendments

AusCheck Act 2007

1 Subsection 4(1)

Insert:

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

2 After paragraph 8(1)(b)

Insert:

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

Security of Critical Infrastructure Act 2018

3 After paragraph 3(b)

Insert:

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

(d) imposing enhanced cyber security obligations on relevant entities for systems of national significance in order to improve their preparedness for, and ability to respond to, cyber security incidents; and

4 Section 4

After paragraph (a) of the paragraph beginning "The framework consists of the following:", insert:

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

5 Section 4

After paragraph (c) of the paragraph beginning "The framework consists of the following:", insert:

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

6 Section 4

After the paragraph beginning "The Minister may privately declare", insert:

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

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

After "market", insert "or system".

8 Section 5

Insert:

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

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

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

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

Repeal the paragraphs, substitute:

(a) a service that:
  (i) enables end-users to store or back-up data; and
  (ii) is provided on a commercial basis; or

(b) a data processing service that:
  (i) involves the use of one or more computers; and

(ii) is provided on a commercial basis.

10 Section 5

Insert:

designated officer has the meaning given by section 30DQ.

evaluation report has the meaning given by section 30CS.

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

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

Repeal the definition, substitute:

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

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

(b) critical to:

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

(ii) national security; or

(iii) the defence of Australia.

12 Section 5

Insert:

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

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

Add:

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

(s) subsection 52D(4).

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

Insert:

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

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

Insert:

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

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

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

Insert:

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

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

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

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

Repeal the definition.

18 Section 5

Insert:

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

19 Section 5

Insert:

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

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

Omit "and 12N", substitute ", 12N, 30AG, 30CB, 30CM, 30CR, 30CU and 30CW".

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

Omit "and 12N", substitute ", 12N, 30AG, 30CB, 30CM, 30CR, 30CU and 30CW".

22 Section 5

Insert:

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

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

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

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

vulnerability assessment has the meaning given by section 30CY.

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

23 At the end of section 8G

Add:

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

(a) the impact (whether direct or indirect) of the incident on the availability of the system;
(b) the impact (whether direct or indirect) of the incident on the integrity of the system;
(c) the impact (whether direct or indirect) of the incident on the reliability of the system;
(d) the impact (whether direct or indirect) of the incident on the confidentiality of:
(i) information about the system; or
(ii) if information is stored in the system—the information; or
(iii) if the system is computer data—the computer data.

24 Paragraph 12F(1)(b)

Omit "wholly or primarily".

25 Paragraph 12F(1)(b)

Omit "on a commercial basis".

26 After paragraph 12F(1)(c)

Insert:

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

27 Paragraph 12F(2)(b)

Omit "wholly or primarily".

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

Omit "on a commercial basis".

29 After paragraph 12F(2)(c)

Insert:

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

30 Paragraph 12J(1)(a)

Omit "a registrable superannuation entity", substitute "an RSE licensee".

31 Paragraph 12J(2)(a)

Omit "registrable superannuation entities", substitute "RSE licensees".

32 Paragraph 12J(2)(b)

Omit "a registrable superannuation entity", substitute "an RSE licensee".

33 After paragraph 12KA(1)(b)

Insert:

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

34 At the end of section 12KA

Add:

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

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

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

35 Paragraph 12L(6)(a)

Omit "registrable superannuation entity", substitute "RSE licensee".

36 At the end of section 12L

Add:

System of national significance

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

37 After Part 2

Insert:

Part 2A—Critical infrastructure risk management programs

30AA Simplified outline of this Part

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

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

30AB Application of this Part

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

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

(b) both:

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

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

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

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

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

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

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

30ABA Consultation—rules

Scope

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

Consultation

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

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

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

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

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

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

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

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

(a) adopt; and

(b) maintain;

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

Civil penalty: 200 penalty units.

30AD Compliance with critical infrastructure risk management program

If:

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

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

the entity must comply with:

(c) the critical infrastructure risk management program; or

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

Civil penalty: 200 penalty units.

30AE Review of critical infrastructure risk management program

If:

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

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

the entity must review the program on a regular basis.

Civil penalty: 200 penalty units.

30AF Update of critical infrastructure risk management program

If:

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

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

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

Civil penalty: 200 penalty units.

30AG Responsible entity must submit annual report

Scope

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

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

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

Annual report

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

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

(b) in any other case—the Secretary;

a report that:

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

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

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

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

(i) identifies the hazard; and

(ii) evaluates the effectiveness of the program in mitigating the significant relevant impact of the hazard on the assets concerned; and

(iii) if the program was varied during the financial year as a result of the occurrence of the hazard—outlines the variation; and

(e) is in the approved form; and

(f) if the entity has a board, council or other governing body—is approved by the board, council or other governing body, as the case requires.

Civil penalty: 150 penalty units.

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

30AH Critical infrastructure risk management program

(1) A ***critical infrastructure risk management program*** is a written program:

(a) that applies to a particular entity that is the responsible entity for one or more critical infrastructure assets; and

(b) the purpose of which is to do the following for each of those assets:

(i) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;

(ii) so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring;

(iii) so far as it is reasonably practicable to do so—mitigate the relevant impact of such a hazard on the asset; and

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

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

(a) may be of general application; or

(b) may relate to one or more specified critical infrastructure assets.

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

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

(4) Rules made for the purposes of paragraph (1)(c) may require that a critical infrastructure risk management program include one or more provisions that permit a background check of an individual to be conducted under the AusCheck scheme.

(5) Subsection (4) does not limit paragraph (1)(c).

(6) In specifying requirements in rules made for the purposes of paragraph (1)(c), the Minister must have regard to the following matters:

(a) any existing regulatory system of the Commonwealth, a State or a Territory that imposes obligations on responsible entities;

(b) the costs that are likely to be incurred by responsible entities in complying with those rules;

(c) the reasonableness and proportionality of the requirements in relation to the purpose referred to in paragraph (1)(b);

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

(7) For the purposes of this section, in determining whether a risk is a material risk, regard must be had to:

(a) the likelihood of the hazard occurring; and

(b) the relevant impact of the hazard on the asset if the hazard were to occur.

(8) The rules may provide that a specified risk is taken to be a material risk for the purposes of this section.

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

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

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

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

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

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

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

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

30AJ Variation of critical infrastructure risk management program

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

30AK Revocation of adoption of critical infrastructure risk management program

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

(a) revoking that adoption; and

(b) adopting another critical infrastructure risk management program that applies to the entity.

30AL Consultation—rules

Scope

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

Consultation

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

(3) Subsection (2) does not apply if:
  (a) the Minister is satisfied that there is an imminent threat that a hazard will have a significant relevant impact on a critical infrastructure asset; or
  (b) the Minister is satisfied that a hazard has had, or is having, a significant relevant impact on a critical infrastructure asset.

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

30AM Review of rules

Scope

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

Review of rules

(2) The Secretary must:

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

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

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

(d) give the Minister:

(i) a report of the review; and

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

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

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

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

(ii) inviting persons to make submissions to the Secretary about the rules or amendments concerned within 28 days after the notice is published; and

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

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

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

Minister to table statement of findings

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

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

Scope

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

Application, adoption or incorporation of a law of a State or Territory

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

Application, adoption or incorporation of a standard

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

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

38 At the end of subsection 30BE

Add:

(3) If:

(a) an entity is or was subject to a requirement under section 30BC or 30BD; and

(b) the entity is or was a member of a related company group;

then:

(c) another member of the related company group is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith for the purposes of ensuring or facilitating compliance with the requirement; and

(d) an officer, employee or agent of another member of the related company group is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith for the purposes of ensuring or facilitating compliance with the requirement.

(4) If:

(a) an entity (the ***first entity***) is or was subject to a requirement under section 30BC or 30BD; and

(b) another entity (the ***contracted service provider***) is or was:

(i) a party to a contract with the first entity; and

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

then:

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

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

39 After Part 2B

Insert:

Part 2C—Enhanced cyber security obligations

Division 1—Simplified outline of this Part

30CA Simplified outline of this Part

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

- 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

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

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

30CC Revocation of determination

Scope

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

Power to revoke determination

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

Application of the Acts Interpretation Act 1901

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

Subdivision B—Statutory incident response planning obligations

30CD Responsible entity must have an incident response plan

If:
(a) an entity is the responsible entity for a system of national significance; and
(b) the statutory incident response planning obligations apply to the entity in relation to:
(i) the system; and
(ii) cyber security incidents;
the entity must:

(c) adopt; and
(d) maintain;

an incident response plan that applies to the entity in relation to:

(e) the system; and
(f) cyber security incidents.

Civil penalty: 200 penalty units.

30CE Compliance with incident response plan

If:

(a) an entity is the responsible entity for a system of national significance; and
(b) the entity has adopted an incident response plan that applies to the entity;

the entity must comply with:

(c) the incident response plan; or
(d) if the plan has been varied on one or more occasions—the plan as varied.

Civil penalty: 200 penalty units.

30CF Review of incident response plan

If:

(a) an entity is the responsible entity for a system of national significance; and
(b) the entity has adopted an incident response plan that applies to the entity;

the entity must review the plan on a regular basis.

Civil penalty: 200 penalty units.

30CG Update of incident response plan

If:

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

(b) the entity has adopted an incident response plan that applies to the entity;

the entity must take all reasonable steps to ensure that the plan is up to date.

Civil penalty: 200 penalty units.

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

(1) If:

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

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

the entity must:

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

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

Civil penalty: 200 penalty units.

(2) If:

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

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

the entity must:

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

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

Civil penalty: 200 penalty units.

30CJ Incident response plan

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

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

(b) that relates to the system; and

(c) that relates to cyber security incidents; and

(d) the purpose of which is to plan for responding to cyber security incidents that could have a relevant impact on the system; and

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

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

(a) may be of general application; or

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

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

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

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

30CK Variation of incident response plan

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

30CL Revocation of adoption of incident response plan

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

(a) revoking that adoption; and

(b) adopting another incident response plan that applies to the entity.

Division 3—Cyber security exercises

30CM Requirement to undertake cyber security exercise

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

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

(2) The Secretary may, by written notice given to an entity that is the responsible entity for a system of national significance, require the entity to:
(a) undertake a cyber security exercise in relation to:
(i) the system; and
(ii) one or more specified types of cyber security incidents; and
(b) do so within the period specified in the notice.

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

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

(5) Before giving a notice to an entity under subsection (1) or (2) in relation to a system of national significance, the Secretary must consult:
(a) the entity; and

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

30CN Cyber security exercise

(1) A ***cyber security exercise*** is an exercise:

(a) that is undertaken by the responsible entity for a system of national significance; and

(b) that relates to the system; and

(c) that either:

(i) relates to all types of cyber security incidents; or

(ii) relates to one or more specified types of cyber security incidents; and

(d) if the exercise relates to all types of cyber security incidents—the purpose of which is to:

(i) test the entity's ability to respond appropriately to all types of cyber security incidents that could have a relevant impact on the system; and

(ii) test the entity's preparedness to respond appropriately to all types of cyber security incidents that could have a relevant impact on the system; and

(iii) test the entity's ability to mitigate the relevant impacts that all types of cyber security incidents could have on the system; and

(e) if the exercise relates to one or more specified types of cyber security incidents—the purpose of which is to:

(i) test the entity's ability to respond appropriately to those types of cyber security incidents that could have a relevant impact on the system; and

(ii) test the entity's preparedness to respond appropriately to those types of cyber security incidents that could have a relevant impact on the system; and

(iii) test the entity's ability to mitigate the relevant impacts that those types of cyber security incidents could have on the system; and

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

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

(a) may be of general application; or

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

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

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

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

30CP Compliance with requirement to undertake cyber security exercise

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

Civil penalty: 200 penalty units.

30CQ Internal evaluation report

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

(a) do both of the following:

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

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

(b) do so:

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

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

Civil penalty: 200 penalty units.

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

30CR External evaluation report

Scope

(1) This section applies if an entity has undertaken a cyber security exercise under section 30CM, and:

(a) all of the following conditions are satisfied:

(i) the entity has prepared, or purported to prepare, an evaluation report under section 30CQ relating to the exercise;

(ii) the entity has given a copy of the report to the Secretary;

(iii) the Secretary has reasonable grounds to believe that the report was not prepared appropriately; or

(b) the entity has contravened section 30CQ.

Requirement

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

(a) appoint an external auditor; and

(b) arrange for the external auditor to prepare an evaluation report (the ***new evaluation report***) relating to the exercise; and

(c) arrange for the external auditor to give the new evaluation report to the entity; and

(d) give the Secretary a copy of the new evaluation report within:

(i) the period specified in the notice; or

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

(3) The notice must specify:

(a) the matters to be covered by the new evaluation report; and

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

Consultation

(4) Before giving a notice to an entity under this section in connection with a cyber security exercise that relates to a system of national significance, the Secretary must consult:

(a) the entity; and

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

Eligibility for appointment as an external auditor

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

Compliance

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

Civil penalty: 200 penalty units.

Immunity

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

30CS Meaning of *evaluation report*

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

(a) if the exercise relates to all types of cyber security incidents—the purpose of which is to:

(i) evaluate the entity's ability to respond appropriately to all types of cyber security incidents that could have a relevant impact on the system; and

(ii) evaluate the entity's preparedness to respond appropriately to all types of cyber security incidents that could have a relevant impact on the system; and

(iii) evaluate the entity's ability to mitigate the relevant impacts that all types of cyber security incidents could have on the system; and

(b) if the exercise relates to one or more specified types of cyber security incidents—the purpose of which is to:

(i) evaluate the entity's ability to respond appropriately to those types of cyber security incidents that could have a relevant impact on the system; and

(ii) evaluate the entity's preparedness to respond appropriately to those types of cyber security incidents that could have a relevant impact on the system; and

(iii) evaluate the entity's ability to mitigate the relevant impacts that those types of cyber security incidents could have on the system; and

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

30CT External auditors

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

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

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

Division 4—Vulnerability assessments

30CU Requirement to undertake vulnerability assessment

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

(a) undertake, or cause to be undertaken, a vulnerability assessment in relation to:
(i) the system; and
(ii) all types of cyber security incidents; and
(b) do so within the period specified in the notice.

(2) The Secretary may, by written notice given to an entity that is the responsible entity for a system of national significance, require the entity to:
(a) undertake, or cause to be undertaken, a vulnerability assessment in relation to:
(i) the system; and
(ii) one or more specified types of cyber security incidents; and
(b) do so within the period specified in the notice.

(3) Before giving a notice to an entity under subsection (1) or (2) in relation to the system of national significance, the Secretary must consult:
(a) the entity; and
(b) if there is a relevant Commonwealth regulator that has functions relating to the security of that system—the relevant Commonwealth regulator.

30CV Compliance with requirement to undertake a vulnerability assessment

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

Civil penalty: 200 penalty units.

30CW Designated officers may undertake a vulnerability assessment

Scope

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

(b) either:

(i) the Secretary has reasonable grounds to believe that if the entity were to be given a notice under subsection 30CU(1) or (2), the entity would not be capable of complying with the notice; or

(ii) the entity has not complied with a notice given to the entity under subsection 30CU(1) or (2).

Request

(2) The Secretary may give a designated officer a written request to:

(a) undertake a vulnerability assessment in relation to:

(i) the system; and

(ii) all types of cyber security incidents; and

(b) do so within the period specified in the request.

(3) The Secretary may give a designated officer a written request to:

(a) undertake a vulnerability assessment in relation to:

(i) the system; and

(ii) one or more specified types of cyber security incidents; and

(b) do so within the period specified in the request.

(4) Before giving a request under subsection (2) or (3) in relation to the system of national significance, the Secretary must consult:

(a) the entity; and

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

Requirement

(5) If a request under subsection (2) or (3) is given to a designated officer, the Secretary may, by written notice given to the entity, require the entity to do any or all of the following things:

(a) provide the designated officer with access to premises for the purposes of undertaking the vulnerability assessment;

(b) provide the designated officer with access to computers for the purposes of undertaking the vulnerability assessment;

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

Notification of request

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

30CX Compliance with requirement to provide reasonable assistance etc.

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

Civil penalty: 200 penalty units.

30CY Vulnerability assessment

(1) A ***vulnerability assessment*** is an assessment:

(a) that relates to a system of national significance; and

(b) that either:

(i) relates to all types of cyber security incidents; or

(ii) relates to one or more specified types of cyber security incidents; and

(c) if the assessment relates to all types of cyber security incidents—the purpose of which is to test the vulnerability of the system to all types of cyber security incidents; and

(d) if the assessment relates to one or more specified types of cyber security incidents—the purpose of which is to test the vulnerability of the system to those types of cyber security incidents; and

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

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

(a) may be of general application; or

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

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

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

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

30CZ Vulnerability assessment report

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

(a) do both of the following:

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

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

(b) do so:

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

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

Civil penalty: 200 penalty units.

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

(a) do both of the following:

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

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

(b) do so:

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

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

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

entity in civil proceedings relating to a contravention of a civil penalty provision of this Act (other than subsection (1)).

30DA Meaning of *vulnerability assessment report*

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

(a) if the assessment relates to all types of cyber security incidents—the purpose of which is to assess the vulnerability of the system to all types of cyber security incidents; and

(b) if the assessment relates to one or more specified types of cyber security incidents—the purpose of which is to assess the vulnerability of the system to those types of cyber security incidents; and

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

Division 5—Access to system information

Subdivision A—System information reporting notices

30DB Secretary may require periodic reporting of system information

Scope

(1) This section applies if:

(a) a computer:

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

(ii) is a system of national significance; and

(b) the Secretary believes on reasonable grounds that a relevant entity for the system of national significance is technically capable of preparing periodic reports consisting of information that:

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

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

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

Requirement

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

(a) prepare periodic reports that:

(i) consist of any such information; and

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

(b) prepare those periodic reports:

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

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

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

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

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

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

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

Matters to be set out in notice

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

Other powers not limited

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

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

Scope

(1) This section applies if:

(a) a computer:

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

(ii) is a system of national significance; and

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

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

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

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

Requirement

(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:

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

(b) prepare that report:

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

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

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

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

(4) In deciding whether to give a system information event-based reporting notice to the entity, the Secretary must have regard to:

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

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

Matters to be set out in notice

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

Other powers not limited

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

30DD Consultation

Before giving:

(a) a system information periodic reporting notice; or

(b) a system information event-based reporting notice;

to a relevant entity for a system of national significance, the Secretary must consult:

(c) the relevant entity; and

(d) if the relevant entity is not the responsible entity for the system of national significance—the responsible entity for the system of national significance.

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

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

(a) comes into force:

(i) when it is given; or

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

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

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

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

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

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

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

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

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

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

An entity must comply with:

(a) a system information periodic reporting notice; or

(b) a system information event-based reporting notice;

to the extent that the entity is capable of doing so.

Civil penalty: 200 penalty units.

30DG Self-incrimination etc.

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

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

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

30DH Admissibility of report etc.

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

(a) the report; or

(b) giving the report;

is not admissible in evidence against an entity:

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

(d) in civil proceedings other than proceedings for recovery of a penalty in relation to a contravention of section 30DF.

Subdivision B—System information software

30DJ Secretary may require installation of system information software

Scope

(1) This section applies if:

(a) a computer:

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

(ii) is a system of national significance; and

(b) the Secretary believes on reasonable grounds that a relevant entity for the system of national significance would not be technically capable of preparing reports under section 30DB or 30DC consisting of information that:

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

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

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

Requirement

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

(a) both:

(i) install a specified computer program on the computer; and

(ii) do so within the period specified in the notice; and

(b) maintain the computer program installed in accordance with paragraph (a); and

(c) take all reasonable steps to ensure that the computer is continuously supplied with an internet carriage service that enables the computer program to function.

(3) A notice under subsection (2) is to be known as a ***system information software notice***.

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

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

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

(5) A computer program may only be specified in a system information software notice if the purpose of the computer program is to:

(a) collect and record information that:

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

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

(iii) is not personal information (within the meaning of the *Privacy Act 1988*); and

(b) cause the information to be transmitted electronically to ASD.

Matters to be set out in notice

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

Other powers not limited

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

30DK Consultation

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

(a) the relevant entity; and

(b) if the relevant entity is not the responsible entity for the system of national significance—the responsible entity for the system of national significance.

30DL Duration of system information software notice

(1) A system information software notice:

(a) comes into force:

(i) when it is given; or

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

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

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

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

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

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

30DM Compliance with system information software notice

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

Civil penalty: 200 penalty units.

30DN Self-incrimination etc.

(1) An entity is not excused from complying with a system information software notice on the ground that complying with the notice might tend to incriminate the entity.

(2) If, at general law, an individual would otherwise be able to claim the privilege against self-exposure to a penalty (other than a penalty for an offence) in relation to complying with a system information software notice, the individual is not excused from complying with the notice on that ground.

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

30DP Admissibility of information etc.

If:

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

(b) information is transmitted to ASD as a result of the operation of the computer program;

the information is not admissible in evidence against an entity:

(c) in criminal proceedings; or

(d) in civil proceedings other than proceedings for recovery of a penalty in relation to a contravention of section 30DM.

Division 6—Designated officers

30DQ Designated officer

(1) A ***designated officer*** is an individual appointed by the Secretary, in writing, to be a designated officer for the purposes of this Act.

(2) The Secretary must not appoint an individual under subsection (1) unless:
  (a) the individual is a Departmental employee; or
  (b) both:
    (i) the individual is a staff member of ASD; and
    (ii) the Director-General of ASD has agreed to the appointment.

(3) The Secretary may, in writing, declare that each Departmental employee included in a specified class of Departmental employees is a designated officer.

(4) The Secretary may, in writing, declare that each staff member of ASD included in a specified class of staff members of ASD is a designated officer.

(5) The Secretary must not make a declaration under subsection (4) unless the Director-General of ASD has agreed to the declaration.

(6) For the purposes of this section, ***Departmental employee*** means an APS employee in the Department.

(7) For the purposes of this section, ***staff member of ASD*** has the same meaning as in the *Intelligence Services Act 2001*.

(8) A declaration under this section is not a legislative instrument.

40 After section 35

Insert:

35AAA Directions prevail over inconsistent critical infrastructure risk management programs

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

41 At the end of subsection 35AAB

Add:

(3) If:

(a) an entity is or was subject to a direction under subsection 32(2); and

(b) the entity is or was a member of a related company group;

then:

(c) another member of the related company group is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith for the purposes of ensuring or facilitating compliance with the direction; and

(d) an officer, employee or agent of another member of the related company group is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith for the purposes of ensuring or facilitating compliance with the direction.

(4) If:

(a) an entity (the ***first entity***) is or was subject to a direction under subsection 32(2); and

(b) another entity (the ***contracted service provider***) is or was:

(i) a party to a contract with the first entity; and

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

then:

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

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

42 After section 35AT

Insert:

35AU Directions prevail over inconsistent critical infrastructure risk management programs

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

43 At the end of subsection 35AW

Add:

(3) If:

(a) an entity is or was subject to a direction given under section 35AQ; and

(b) the entity is or was a member of a related company group;

then:

(c) another member of the related company group is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith for the purposes of ensuring or facilitating compliance with the direction; and

(d) an officer, employee or agent of another member of the related company group is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith for the purposes of ensuring or facilitating compliance with the direction.

(4) If:

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

(b) another entity (the ***contracted service provider***) is or was:

(i) a party to a contract with the first entity; and

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

then:

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

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

44 At the end of subsection 35BB

Add:

(6) If:

(a) an entity is or was subject to a requirement under subsection (1); and

(b) the entity is or was a member of a related company group;

then:

(c) another member of the related company group is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith for the purposes of ensuring or facilitating compliance with the requirement; and

(d) an officer, employee or agent of another member of the related company group is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith for the purposes of ensuring or facilitating compliance with the requirement.

(7) If:

(a) an entity (the ***first entity***) is or was subject to a requirement under subsection (1); and

(b) another entity (the ***contracted service provider***) is or was:

(i) a party to a contract with the first entity; and

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

then:

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

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

45 After section 43D

Insert:

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

(1) An entity may disclose protected information if:

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

(b) the entity discloses the protected information to:

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

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

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

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

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

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

(2) An entity may disclose protected information if:

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

(b) the protected information is covered by:

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

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

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

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

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

(3) An entity may disclose protected information if:

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

(b) the protected information is not covered by:

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

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

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

46 Subsection 46(2)

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

47 Paragraph 46(4)(b)

Repeal the paragraph.

48 After paragraph 51(2A)(a)

Insert:

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

49 After Part 6

Insert:

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

Division 1—Simplified outline of this Part

52A Simplified outline of this Part

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

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

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.

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

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

52B Declaration of systems of national significance by the Minister

(1) The Minister may, in writing, declare a particular asset to be a system of national significance if:

(a) the asset is a critical infrastructure asset; and

(b) the Minister is satisfied that the asset is of national significance.

(2) In determining whether an asset is of national significance for the purposes of subsection (1), the Minister must have regard to:

(a) the consequences that would arise for:

(i) the social or economic stability of Australia or its people; or

(ii) the defence of Australia; or

(iii) national security;

if a hazard were to occur that had a significant relevant impact on the asset; and

(b) if the Minister is aware of one or more interdependencies between the asset and one or more other critical infrastructure assets—the nature and extent of those interdependencies; and

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

(3) The Minister must notify the following of the declaration, in writing, within 30 days after making the declaration in relation to an asset:

(a) each reporting entity for the asset;

(b) if the asset is a tangible asset located (wholly or partly) in a State, the Australian Capital Territory or the Northern Territory—the First Minister of the State, the Australian Capital Territory or the Northern Territory, as the case requires.

(4) A declaration under subsection (1) is not a legislative instrument.

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

52C Consultation—declaration

(1) Before making a declaration under section 52B in relation to an asset, the Minister must give the responsible entity for the asset a notice:
  (a) setting out the proposed declaration; and
  (b) inviting the entity to make submissions to the Minister about the proposed declaration within:
    (i) 28 days after the notice is given; or
    (ii) if a shorter period is specified in the notice—that shorter period.

(2) The Minister must consider any submissions received within:
  (a) the 28-day period mentioned in subparagraph (1)(b)(i); or
  (b) if a shorter period is specified in the notice—that shorter period.

(3) The Minister must not specify a shorter period in the notice unless the Minister is satisfied that the shorter period is necessary due to urgent circumstances.

(4) The notice must set out the reasons for making the declaration, unless the Minister is satisfied that doing so would be prejudicial to security.

52D Notification of change to reporting entities for asset

Scope

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

Notification

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

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

(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).

Civil penalty: 150 penalty units.

(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).

(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.

52E Review of declaration

Scope

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

Request

(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.

Requirement

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

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

(b) give the Minister:

(i) a report of the review; and

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

(4) The review must be undertaken in consultation with the responsible entity for the asset.

(5) In reviewing whether the asset is of national significance, the Secretary must have regard to:

(a) the consequences that would arise for:

(i) the social or economic stability of Australia or its people; or

(ii) the defence of Australia; or

(iii) national security;

if a hazard were to occur that had a significant relevant impact on the asset; and

(b) if the Secretary is aware of one or more interdependencies between the asset and one or more other critical infrastructure assets—the nature and extent of those interdependencies; and

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

Limit

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

52F Revocation of determination

Scope

(1) This section applies if:

(a) a declaration under subsection 52B(1) is in force in relation to an asset; and

(b) the Minister is no longer satisfied that the asset is of national significance.

Duty to revoke declaration

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

Revocation is not a legislative instrument

(3) A revocation of the declaration is not a legislative instrument.

Application of Acts Interpretation Act 1901

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

50 After paragraph 60(2)(e)

Insert:

(f) the number of annual reports given under section 30AG during the financial year; and

(g) the number of annual reports given under section 30AG during the financial year that included a statement to the effect that a critical infrastructure risk management program was up to date at the end of the financial year; and

51 After paragraph 60(2)(i)

Insert:

(j) the number of notices given to entities under section 30CB during the financial year; and

(k) the number of notices given to entities under section 30CM during the financial year; and

(l) the number of notices given to entities under section 30CU during the financial year; and

(m) the number of notices given to entities under Division 5 of Part 2C during the financial year; and

52 At the end of subsection 60(2)

Add:

; and (r) the number of declarations of assets as systems of national significance that were made under section 52B during the financial year.