Security of Critical Infrastructure Act 2018

No. 29, 2018

Compilation No. 4

Compilation date:	2 April 2022
Includes amendments up to:	Act No. 33, 2022
Registered:	2 May 2022

Prepared by the Office of Parliamentary Counsel, Canberra

Authorised Version C2022C00160 registered 02/05/2022

About this compilation

This compilation

This is a compilation of the *Security of Critical Infrastructure Act 2018* that shows the text of the law as amended and in force on 2 April 2022 (the ***compilation date***).

The notes at the end of this compilation (the ***endnotes***) include information about amending laws and the amendment history of provisions of the compiled law.

Uncommenced amendments

The effect of uncommenced amendments is not shown in the text of the compiled law. Any uncommenced amendments affecting the law are accessible on the Legislation Register (www.legislation.gov.au). The details of amendments made up to, but not commenced at, the compilation date are underlined in the endnotes. For more information on any uncommenced amendments, see the series page on the Legislation Register for the compiled law.

Application, saving and transitional provisions for provisions and amendments

If the operation of a provision or amendment of the compiled law is affected by an application, saving or transitional provision that is not included in this compilation, details are included in the endnotes.

Editorial changes

For more information about any editorial changes made in this compilation, see the endnotes.

Modifications

If the compiled law is modified by another law, the compiled law operates as modified but the modification does not amend the text of the law. Accordingly, this compilation does not show the text of the compiled law as modified. For more information on any modifications, see the series page on the Legislation Register for the compiled law.

Self-repealing provisions

If a provision of the compiled law has been repealed in accordance with a provision of the law, details are included in the endnotes.

Contents

Part 1—Preliminary 1

Division 1—Preliminary 1

1 Short title 1
2 Commencement 1
3 Object 2
4 Simplified outline of this Act 2

Division 2—Definitions 5

5 Definitions 5
6 Meaning of *interest and control information* 30
7 Meaning of *operational information* 32
8 Meaning of *direct interest holder* 33
8A Meaning of *influence or control* 35
8B Meaning of *associate* 36
8C Meanings of *subsidiary* and *holding entity* 37
8D Meaning of *critical infrastructure sector* 38
8E Meaning of *critical infrastructure sector asset* 38
8F Critical infrastructure sector for a critical infrastructure asset 40
8G Meaning of *relevant impact* 40
9 Meaning of *critical infrastructure asset* 41
10 Meaning of *critical electricity asset* 44
11 Meaning of *critical port* 45
12 Meaning of *critical gas asset* 46
12A Meaning of *critical liquid fuel asset* 46
12B Meaning of *critical freight infrastructure asset* 47
12C Meaning of *critical freight services asset* 50
12D Meaning of *critical financial market infrastructure asset* 50
12E Meaning of *critical broadcasting asset* 54
12F Meaning of *critical data storage or processing asset* 54
12G Meaning of *critical banking asset* 56
12H Meaning of *critical insurance asset* 57
12J Meaning of *critical superannuation asset* 60
12K Meaning of *critical food and grocery asset* 60
12KA Meaning of *critical domain name system* 61
12L Meaning of *responsible entity* 62
12M Meaning of *cyber security incident* 69

Authorised Version C2022C00160 registered 02/05/2022

12N Meaning of *unauthorised access, modification or impairment* ... 70
12P Examples of responding to a cyber security incident ... 71

Division 3—Constitutional provisions and application of this Act 72
13 Application of this Act ... 72
14 Extraterritoriality ... 73
15 This Act binds the Crown ... 73
16 Concurrent operation of State and Territory laws ... 73
17 State constitutional powers ... 73

Part 2—Register of Critical Infrastructure Assets 74

Division 1—Introduction 74
18 Simplified outline of this Part ... 74
18A Application of this Part ... 74
18AA Consultation—rules ... 75

Division 2—Register of Critical Infrastructure Assets 76
19 Secretary must keep Register ... 76
20 Secretary may add information to Register ... 76
21 Secretary may correct or update information in the Register ... 76
22 Register not to be made public ... 76

Division 3—Obligation to give information and notify of events 77
23 Initial obligation to give information ... 77
24 Ongoing obligation to give information and notify of events ... 78
25 Information that is not able to be obtained ... 80
26 Meaning of *notifiable event* ... 80
27 Rules may exempt from requirement to give notice or information ... 81

Division 4—Giving of notice or information by agents etc. 82
28 Requirement for executors and administrators to give notice or information for individuals who die ... 82
29 Requirement for corporate liquidators etc. to give notice or information ... 82
30 Agents may give notice or information ... 82

Part 2A—Critical infrastructure risk management programs 83
30AA Simplified outline of this Part ... 83
30AB Application of this Part ... 83
30ABA Consultation—rules ... 85

Authorised Version C2022C00160 registered 02/05/2022

30AC Responsible entity must have a critical infrastructure risk management program 85
30AD Compliance with critical infrastructure risk management program 86
30AE Review of critical infrastructure risk management program 86
30AF Update of critical infrastructure risk management program 86
30AG Responsible entity must submit annual report 87
30AH Critical infrastructure risk management program 88
30AJ Variation of critical infrastructure risk management program 91
30AK Revocation of adoption of critical infrastructure risk management program 91
30AKA Responsible entity must have regard to certain matters in deciding whether to adopt or vary critical infrastructure risk management program etc. 91
30AL Consultation—rules made for the purposes of section 30AH or 30AKA 93
30AM Review of rules 94
30AN Application, adoption or incorporation of a law of a State or Territory etc. 95
30ANA Application, adoption or incorporation of certain documents 95
30ANB Consultation—rules made for the purposes of paragraph 30ANA(2)(f) 96
30ANC Disallowance of rules 97

Part 2AA—Reporting obligations relating to certain assets that are not covered by a critical infrastructure risk management program 99

30AP Simplified outline of this Part 99
30AQ Reporting obligations relating to certain assets that are not covered by a critical infrastructure risk management program 99

Part 2B—Notification of cyber security incidents 101

30BA Simplified outline of this Part 101
30BB Application of this Part 101
30BBA Consultation—rules 102
30BC Notification of critical cyber security incidents 102
30BD Notification of other cyber security incidents 104
30BE Liability 106
30BEA Significant impact 107
30BEB Consultation—rules 108
30BF Relevant Commonwealth body 108

Authorised Version C2022C00160 registered 02/05/2022

Part 2C—Enhanced cyber security obligations 110

Division 1—Simplified outline of this Part 110

30CA Simplified outline of this Part 110

Division 2—Statutory incident response planning obligations 111

Subdivision A—Application of statutory incident response planning obligations 111

30CB Application of statutory incident response planning obligations—determination by the Secretary 111

30CC Revocation of determination 112

Subdivision B—Statutory incident response planning obligations 112

30CD Responsible entity must have an incident response plan 112

30CE Compliance with incident response plan 113

30CF Review of incident response plan 113

30CG Update of incident response plan 114

30CH Copy of incident response plan must be given to the Secretary 114

30CJ Incident response plan 115

30CK Variation of incident response plan 115

30CL Revocation of adoption of incident response plan 115

Division 3—Cyber security exercises 116

30CM Requirement to undertake cyber security exercise 116

30CN Cyber security exercise 117

30CP Compliance with requirement to undertake cyber security exercise 119

30CQ Internal evaluation report 119

30CR External evaluation report 119

30CS Meaning of *evaluation report* 121

30CT External auditors 122

Division 4—Vulnerability assessments 123

30CU Requirement to undertake vulnerability assessment 123

30CV Compliance with requirement to undertake a vulnerability assessment 124

30CW Designated officers may undertake a vulnerability assessment 124

30CX Compliance with requirement to provide reasonable assistance etc. 125

30CY Vulnerability assessment 126

30CZ Vulnerability assessment report 126

Authorised Version C2022C00160 registered 02/05/2022

30DA Meaning of *vulnerability assessment report* 127

Division 5—Access to system information 129

Subdivision A—System information reporting notices 129

30DB Secretary may require periodic reporting of system information 129

30DC Secretary may require event-based reporting of system information 130

30DD Consultation 132

30DE Duration of system information periodic reporting notice or system information event-based reporting notice 132

30DF Compliance with system information periodic reporting notice or system information event-based reporting notice 133

30DG Self-incrimination etc. 133

30DH Admissibility of report etc. 134

Subdivision B—System information software 134

30DJ Secretary may require installation of system information software 134

30DK Consultation 136

30DL Duration of system information software notice 136

30DM Compliance with system information software notice 137

30DN Self-incrimination etc. 137

30DP Admissibility of information etc. 137

Division 6—Designated officers 138

30DQ Designated officer 138

Part 3—Directions by the Minister 139

Division 1—Simplified outline of this Part 139

31 Simplified outline of this Part 139

Division 2—Directions by the Minister 140

32 Direction if risk of act or omission that would be prejudicial to security 140

33 Consultation before giving direction 141

34 Requirement to comply with direction 142

35 Exception—acquisition of property 142

35AAA Directions prevail over inconsistent critical infrastructure risk management programs 143

35AAB Liability 143

Authorised Version C2022C00160 registered 02/05/2022

Part 3A—Responding to serious cyber security incidents 145

Division 1—Simplified outline of this Part 145

35AA Simplified outline of this Part 145

Division 2—Ministerial authorisation relating to cyber security incident 146

35AB Ministerial authorisation 146

35AC Kinds of acts or things that may be specified in an intervention request 151

35AD Consultation 152

35AE Form and notification of Ministerial authorisation 153

35AF Form of application for Ministerial authorisation 156

35AG Duration of Ministerial authorisation 156

35AH Revocation of Ministerial authorisation 157

35AJ Minister to exercise powers personally 159

Division 3—Information gathering directions 160

35AK Information gathering direction 160

35AL Form of direction 161

35AM Compliance with an information gathering direction 162

35AN Self-incrimination etc. 162

35AP Admissibility of information etc. 162

Division 4—Action directions 163

35AQ Action direction 163

35AR Form of direction 164

35AS Revocation of direction 164

35AT Compliance with direction 165

35AU Directions prevail over inconsistent critical infrastructure risk management programs 165

35AV Directions prevail over inconsistent obligations 165

35AW Liability 166

Division 5—Intervention requests 168

35AX Intervention request 168

35AY Form and notification of request 169

35AZ Compliance with request 170

35BA Revocation of request 171

35BB Relevant entity to assist the authorised agency 172

35BC Constable may assist the authorised agency 174

35BD Removal and return of computers etc. 174

Authorised Version C2022C00160 registered 02/05/2022

35BE Use of force against an individual not authorised 176
35BF Liability 176
35BG Evidentiary certificates 176
35BH Chief executive of the authorised agency to report to the Defence Minister and the Minister 176
35BJ Approved staff members of the authorised agency 177

Division 6—Reports to the Parliamentary Joint Committee on Intelligence and Security 178

35BK Reports to the Parliamentary Joint Committee on Intelligence and Security 178

Part 4—Gathering and using information 179

Division 1—Simplified outline of this Part 179

36 Simplified outline of this Part 179

Division 2—Secretary's power to obtain information or documents 180

37 Secretary may obtain information or documents from entities 180
38 Copies of documents 181
39 Retention of documents 181
40 Self-incrimination 182

Division 3—Use and disclosure of protected information 183

Subdivision A—Authorised use and disclosure 183

41 Authorised use and disclosure—performing functions etc. 183
42 Authorised use and disclosure—other person's functions etc. 183
42A Authorised use and disclosure—development of proposed amendments of this Act etc. 184
43 Authorised disclosure relating to law enforcement 184
43AA Authorised disclosure to Ombudsman official 185
43A Authorised disclosure to IGIS official 185
43B Authorised use and disclosure—Ombudsman official 185
43C Authorised use and disclosure—IGIS official 186
43D Authorised use and disclosure—ASD 186
43E Authorised disclosure of protected information by the entity to whom the information relates 186
44 Secondary use and disclosure of protected information 188

Subdivision B—Offence for unauthorised use or disclosure 188

45 Offence for unauthorised use or disclosure of protected information 188

Authorised Version C2022C00160 registered 02/05/2022

46 Exceptions to offence for unauthorised use or disclosure 189
47 No requirement to provide information 190

Part 5—Enforcement 191

Division 1—Simplified outline of this Part 191
48 Simplified outline of this Part 191

Division 2—Civil penalties, enforceable undertakings and injunctions 192
49 Civil penalties, enforceable undertakings and injunctions 192

Division 3—Monitoring and investigation powers 195
49A Monitoring powers 195
49B Investigation powers 198

Division 4—Infringement notices 201
49C Infringement notices 201

Part 6—Declaration of assets by the Minister 203

Division 1—Simplified outline of this Part 203
50 Simplified outline of this Part 203

Division 2—Declaration of assets by the Minister 204
51 Declaration of assets by the Minister 204
51A Consultation—declaration 205
52 Notification of change to reporting entities for asset 205

Part 6A—Declaration of systems of national significance by the Minister 207

Division 1—Simplified outline of this Part 207
52A Simplified outline of this Part 207

Division 2—Declaration of systems of national significance by the Minister 208
52B Declaration of systems of national significance by the Minister 208
52C Consultation—declaration 209
52D Notification of change to reporting entities for asset 210
52E Review of declaration 210
52F Revocation of determination 212

Authorised Version C2022C00160 registered 02/05/2022

Part 7—Miscellaneous 213

Division 1—Simplified outline of this Part 213

53 Simplified outline of this Part 213

Division 2—Treatment of certain entities 214

53A How certain entities hold interests 214

54 Treatment of partnerships 214

55 Treatment of trusts and superannuation funds that are trusts 215

56 Treatment of unincorporated foreign companies 216

Division 3—Matters relating to Secretary's powers 217

57 Additional power of Secretary 217

58 Assets ceasing to be critical infrastructure assets 217

59 Delegation of Secretary's powers 217

Division 4—Periodic reports, reviews and rules etc. 218

60 Periodic report 218

60AAA Regular reports about consultation 219

60AA Compensation for acquisition of property 220

60AB Service of notices, directions and instruments by electronic means 221

60A Independent review 221

60B Review of this Act 221

61 Rules 222

Endnotes 223

Endnote 1—About the endnotes 223

Endnote 2—Abbreviation key 225

Endnote 3—Legislation history 226

Endnote 4—Amendment history 227

Endnote 5—Editorial changes 236

Authorised Version C2022C00160 registered 02/05/2022

Authorised Version C2022C00160 registered 02/05/2022

An Act to create a framework for managing critical infrastructure, and for related purposes

Part 1—Preliminary

Division 1—Preliminary

1 Short title

This Act is the *Security of Critical Infrastructure Act 2018*.

2 Commencement

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

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this Act	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 3 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	11 July 2018

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.

Authorised Version C2022C00160 registered 02/05/2022

3 Object

The object of this Act is to provide a framework for managing risks relating to critical infrastructure, including by:

(a) improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks; and

(b) facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks; and

(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

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

4 Simplified outline of this Act

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

The framework consists of the following:

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

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

(c) requiring notification of cyber security incidents;

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

Authorised Version C2022C00160 registered 02/05/2022

(e) requiring certain entities relating to a critical infrastructure asset to provide information in relation to the asset, and to notify if certain events occur in relation to the asset;

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

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

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

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

Section 4

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

Authorised Version C2022C00160 registered 02/05/2022

Division 2—Definitions

5 Definitions

In this Act:

ABN has the same meaning as in the *A New Tax System (Australian Business Number) Act 1999*.

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

access to computer data means:

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

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

(i) any other location in the computer; or

(ii) another computer; or

(iii) a data storage device; or

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

(i) a computer; or

(ii) another data storage device.

acquisition of property has the same meaning as in paragraph 51(xxxi) of the Constitution.

adverse security assessment has the same meaning as in Part IV of the *Australian Security Intelligence Organisation Act 1979*.

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

appointed officer, for an unincorporated foreign company, means:

(a) the secretary of the company; or

(b) an officer of the company appointed to hold property on behalf of the company.

approved form means a form approved by the Secretary.

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

ASD means the Australian Signals Directorate.

asset includes:

(a) a system; and

(b) a network; and

(c) a facility; and

(d) a computer; and

(e) a computer device; and

(f) a computer program; and

(g) computer data; and

(h) premises; and

(i) any other thing.

associate has the meaning given by section 8B.

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

associated transmission facility means:

(a) an antenna; or

(b) a combiner; or

(c) a feeder system; or

Authorised Version C2022C00160 registered 02/05/2022

(d) an apparatus; or
(e) an item of equipment; or
(f) a structure; or
(g) a line; or
(h) an electricity cable or wire;

that is associated with a radiocommunications transmitter.

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

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

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

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

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

authorised agency means ASD.

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

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

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

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

broadcasting re-transmission asset means:
(a) a radiocommunications transmitter; or
(b) a broadcasting transmission tower; or
(c) an associated transmission facility;

Authorised Version C2022C00160 registered 02/05/2022

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

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

broadcasting transmission asset means:

(a) a radiocommunications transmitter; or
(b) a broadcasting transmission tower; or
(c) an associated transmission facility;

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

(d) a national broadcasting service; or
(e) a commercial radio broadcasting service; or
(f) a commercial television broadcasting service.

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

business critical data means:

(a) personal information (within the meaning of the *Privacy Act 1988*) that relates to at least 20,000 individuals; or
(b) information relating to any research and development in relation to a critical infrastructure asset; or
(c) information relating to any systems needed to operate a critical infrastructure asset; or
(d) information needed to operate a critical infrastructure asset; or
(e) information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset.

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

civil penalty provision has the same meaning as in the Regulatory Powers Act.

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

commencing day means the day this Act commences.

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

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

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

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

computer means all or part of:

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

computer data means data held in:

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

Authorised Version C2022C00160 registered 02/05/2022

computer device means a device connected to a computer.

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

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

corporate entity means an entity other than an individual.

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

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

critical aviation asset means:

(a) an asset that:
  (i) is used in connection with the provision of an air service; and
  (ii) is owned or operated by an aircraft operator; or

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

(c) an asset that is used by an airport operator in connection with the operation of an airport.

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

critical component of a critical infrastructure asset, means a part of the asset, where absence of, damage to, or compromise of, the part of the asset:

(a) would prevent the proper function of the asset; or

(b) could cause significant damage to the asset;

as assessed by the responsible entity for the asset.

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

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

critical defence capability includes:

(a) materiel; and

(b) technology; and

(c) a platform; and

(d) a network; and

(e) a system; and

(f) a service;

that is required in connection with:

(g) the defence of Australia; or

(h) national security.

critical defence industry asset means an asset that:

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

critical education asset means an asset that:

(a) is owned or operated by an entity that is registered in the Australian university category of the National Register of Higher Education Providers; and

(b) is used in connection with undertaking a program of research that is critical to:

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

(ii) the defence of Australia; or

(iii) national security.

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

critical electricity asset has the meaning given by section 10.

critical energy market operator asset means an asset that:

(a) is owned or operated by:

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

(ii) Power and Water Corporation; or

(iii) Regional Power Corporation; or

(iv) Electricity Networks Corporation; and

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

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

but does not include:

(d) a critical electricity asset; or

(e) a critical gas asset; or

(f) a critical liquid fuel asset.

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

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

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

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

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

critical gas asset has the meaning given by section 12.

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

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

critical infrastructure asset has the meaning given by section 9.

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

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

critical port has the meaning given by section 11.

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

(a) is managed by a single entity; and

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

but does not include a critical aviation asset.

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

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

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

critical telecommunications asset means:

(a) a telecommunications network that is:

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

(ii) used to supply a carriage service; or

(b) a facility (within the meaning of the *Telecommunications Act 1997*) that is:

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

(ii) used to supply a carriage service.

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

critical water asset means one or more water or sewerage systems or networks that:

(a) are managed by a single water utility; and

(b) ultimately deliver services to at least 100,000 water connections or 100,000 sewerage connections.

Authorised Version C2022C00160 registered 02/05/2022

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

critical worker means an individual, where the following conditions are satisfied:

(a) the individual is an employee, intern, contractor or subcontractor of the responsible entity for a critical infrastructure asset to which Part 2A applies;

(b) the absence or compromise of the individual:

(i) would prevent the proper function of the asset; or

(ii) could cause significant damage to the asset;

as assessed by the responsible entity for the asset;

(c) the individual has access to, or control and management of, a critical component of the asset.

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

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

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

data includes information in any form.

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

data storage or processing service means:

(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; or

(c) a service that is specified in the rules.

However, the rules may prescribe that a specified service is not a data storage or processing service.

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

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

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

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

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

designated officer has the meaning given by section 30DQ.

direct interest holder, in relation to an asset, has the meaning given by section 8.

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

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

engage in conduct means:

(a) do an act or thing; or

(b) omit to perform an act or thing.

entity means any of the following:

(a) an individual, whether or not resident in Australia or an Australian citizen;

(b) a body corporate, whether or not formed, or carrying on business, in Australia;

(c) a body politic, whether or not an Australian body politic;

(d) a partnership, whether or not formed in Australia;

(e) a trust, whether or not created in Australia;

(f) a superannuation fund, whether or not created in Australia;

(g) an unincorporated foreign company.

Note: See Division 2 of Part 7 for how this Act applies to partnerships, trusts, superannuation funds and unincorporated foreign companies.

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.

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

First Minister means the Premier of a State, or the Chief Minister of the Australian Capital Territory or the Northern Territory.

food means food for human consumption.

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

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

food or groceries on a commercial basis.

gas means a substance that:

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

Authorised Version C2022C00160 registered 02/05/2022

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

general intensive care unit means an area within a hospital that:
(a) is equipped and staffed so that it is capable of providing to a patient:
  (i) mechanical ventilation for a period of several days; and
  (ii) invasive cardiovascular monitoring; and
(b) is supported by:
  (i) during normal working hours—at least one specialist, or consultant physician, in the specialty of intensive care, who is immediately available, and exclusively rostered, to that area; and
  (ii) at all times—at least one medical practitioner who is present in the hospital and immediately available to that area; and
  (iii) at least 18 hours each day—at least one nurse; and
(c) has admission and discharge policies in operation.

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

grace period, for an asset, means:
(a) for an asset that is, or will be, a critical infrastructure asset at the end of the period of 6 months starting on the commencing day—that 6 month period; or
(b) for an asset that becomes a critical infrastructure asset after the end of the period mentioned in paragraph (a)—the period of 6 months starting on the day the asset becomes a critical infrastructure asset.

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

Authorised Version C2022C00160 registered 02/05/2022

(i) dental (including the profession of a dentist, dental therapist, dental hygienist, dental prosthetist and oral health therapist);
(ii) medical;
(iii) medical radiation practice;
(iv) nursing;
(v) midwifery;
(vi) occupational therapy;
(vii) optometry;
(viii) pharmacy;
(ix) physiotherapy;
(x) podiatry;
(xi) psychology;
(xii) a profession or occupation specified in the rules; and

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

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

holding entity has the meaning given by subsection 8C(2).

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

IGIS official means:

(a) the Inspector-General of Intelligence and Security; or

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

impairment of electronic communication to or from a computer includes:

(a) the prevention of any such communication; and

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

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

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

influence or control has a meaning affected by section 8A.

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

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

interest in an asset means a legal or equitable interest in the asset.

interest and control information, in relation to an entity and an asset, has the meaning given by section 6.

international relations means political, military and economic relations with foreign governments and international organisations.

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

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

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

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

medical supplies includes:

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

Ministerial authorisation means an authorisation under section 35AB.

modification:

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

Authorised Version C2022C00160 registered 02/05/2022

(ii) an addition to the program.

moneylending agreement has the meaning given by subsection 8(3).

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

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

national security means Australia's defence, security or international relations.

notifiable event has the meaning given by section 26.

notification provision means:

(a) subsection 35AE(3); or
(b) subsection 35AE(4); or
(c) subsection 35AE(5); or
(d) subsection 35AE(6); or
(e) subsection 35AE(7); or
(f) subsection 35AE(8); or
(g) subsection 35AH(5); or
(h) subsection 35AH(6); or
(i) subsection 35AH(7); or
(j) subsection 35AY(3); or
(k) subsection 35AY(4); or
(l) subsection 35AY(5); or
(m) subsection 35AY(6); or
(n) subsection 35AY(7); or
(o) subsection 35AY(8); or
(p) subsection 51(3); or
(q) subsection 52(4); or
(r) subsection 52B(3); or
(s) subsection 52D(4).

Authorised Version C2022C00160 registered 02/05/2022

Ombudsman official means:

(a) the Ombudsman; or

(b) a Deputy Commonwealth Ombudsman; or

(c) a person who is a member of the staff referred to in subsection 31(1) of the *Ombudsman Act 1976*.

operational information, in relation to an asset, has the meaning given by section 7.

operator, of an asset, means:

(a) for a critical port—a port facility operator (within the meaning of the *Maritime Transport and Offshore Facilities Security Act 2003*) of a port facility within the port; or

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

Note: For some assets, an operator of the asset is also the responsible entity for the asset.

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

port facility has the same meaning as in the *Maritime Transport and Offshore Facilities Security Act 2003*.

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

protected information means a document or information that:

(a) is obtained by a person in the course of exercising powers, or performing duties or functions, under this Act; or

(b) records or is the fact that an asset is declared under section 51 to be a critical infrastructure asset; or

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

(bb) records or is the fact that the Minister has:

(i) given a Ministerial authorisation; or

(ii) revoked a Ministerial authorisation; or

Authorised Version C2022C00160 registered 02/05/2022

(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 30AQ; or

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

(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

(bi) is, or is included in, a report prepared in compliance with:

(i) a system information periodic reporting notice; or

(ii) a system information event-based reporting notice; or

(bj) records or is the fact that the Secretary has:

(i) given a direction under section 35AK; or

(ii) revoked such a direction; or

(bk) records or is the fact that the Secretary has:

(i) given a direction under section 35AQ; or

(ii) revoked such a direction; or

(bl) records or is the fact that the Secretary has:

(i) given a request under section 35AX; or

(ii) revoked such a request; or

(c) was a document or information to which paragraph (a), (b), (ba), (bb), (bc), (bd), (be), (bf), (bg), (bh), (bi), (bj), (bk) or (bl) applied and is obtained by a person by way of an authorised disclosure under Division 3 of Part 4 or in accordance with section 46.

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

Register means the Register of Critical Infrastructure Assets kept by the Secretary under section 19.

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

Regulatory Powers Act means the *Regulatory Powers (Standard Provisions) Act 2014*.

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

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*.

relevant Commonwealth regulator means:

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

(b) a body that is:

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

(ii) specified in the rules.

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

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

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

(c) is an operator of the asset; or

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

relevant impact has the meaning given by section 8G.

reporting entity, for an asset, means either of the following:

(a) the responsible entity for the asset;

Authorised Version C2022C00160 registered 02/05/2022

(b) a direct interest holder in relation to the asset.

Note: An entity may be both the responsible entity for an asset and a direct interest holder in relation to the asset.

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

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

rules means the rules made by the Minister under section 61.

Secretary means the Secretary of the Department.

security (other than in references to national security):

(a) other than in the definition of ***critical energy market operator asset*** and sections 10, 12, 12A, 12D, 12G, 12H, 12J, 12M, 12N, 30AG, 30AQ, 30CB, 30CM, 30CR, 30CU and 30CW—has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*; and

(b) in the definition of ***critical energy market operator asset*** and sections 10, 12, 12A, 12D, 12G, 12H, 12J, 12M, 12N, 30AG, 30AQ, 30CB, 30CM, 30CR, 30CU and 30CW—has its ordinary meaning.

security regulated port has the same meaning as in the *Maritime Transport and Offshore Facilities Security Act 2003*.

Note: Security regulated ports are declared under section 13 of the *Maritime Transport and Offshore Facilities Security Act 2003*.

senior officer of a corporate entity means:

(a) for a body corporate—a director of the body corporate; or

(b) for a unit trust:

(i) the trustee of which is an individual—the trustee; and

(ii) the trustee of which is a body corporate—a director of the trustee; and

(iii) in any case—any other individual involved in the central management and control of the trust; or

Authorised Version C2022C00160 registered 02/05/2022

(c) an individual who is, or an individual in a group of individuals who are, in a position to determine the investments or policy of the entity or a trustee of the entity; or

(d) an individual who makes, or participates in making, decisions that affect the whole, or a substantial part of, the business of the entity; or

(e) an individual who has the capacity to affect significantly the financial standing of the entity.

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

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

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

(a) position, navigation and timing services in relation to space objects;

(b) space situational awareness services;

(c) space weather monitoring and forecasting;

(d) communications, tracking, telemetry and control in relation to space objects;

(e) remote sensing earth observations from space;

(f) facilitating access to space.

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

subsidiary has the meaning given by subsection 8C(1).

superannuation fund has the meaning given by section 10 of the *Superannuation Industry (Supervision) Act 1993*.

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).

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

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

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

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

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

this Act includes the rules.

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

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

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

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

unincorporated foreign company means a body covered by paragraph (b) of the definition of ***foreign company*** in section 9 of the *Corporations Act 2001*.

vulnerability assessment has the meaning given by section 30CY.

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

water utility means an entity that holds a licence, approval or authorisation (however described), under a law of the Commonwealth, a State or a Territory, to provide water services or sewerage services, or both.

6 Meaning of *interest and control information*

(1) The following information is ***interest and control information*** in relation to an entity (the ***first entity***) and an asset (subject to subsection (3)):

(a) the name of the first entity;

(b) if applicable, the ABN of the first entity, or other similar business number (however described) if the first entity was incorporated, formed or created (however described) outside Australia;

(c) for an entity other than an individual:

(i) the address of the first entity's head office or principal place of business; and

(ii) the country in which the first entity was incorporated, formed or created (however described);

(d) for an entity that is an individual:

(i) the residential address of the first entity; and

(ii) the country in which the first entity usually resides; and

(iii) the country or countries of which the first entity is a citizen;

(e) the type and level of the interest the first entity holds in the asset;

Authorised Version C2022C00160 registered 02/05/2022

(f) information about the influence or control the first entity is in a position to directly or indirectly exercise in relation to the asset;

(g) information about the ability of a person, who has been appointed by the first entity to the body that governs the asset, to directly access networks or systems that are necessary for the operation or control of the asset;

(h) the name of each other entity that is in a position to directly or indirectly influence or control:

(i) the first entity; or

(ii) any entity covered by a previous application of this paragraph;

(ha) in relation to each entity (the ***higher entity***) covered by paragraph (h):

(i) the information in paragraphs (b) to (d), and (e) if appropriate, as if a reference in those paragraphs to the first entity were a reference to the higher entity; and

(ii) information about the influence or control the higher entity is in a position to directly or indirectly exercise in relation to the first entity or any entity covered by paragraph (h);

(i) information prescribed by the rules for the purposes of this paragraph.

Note 1: For example, if Holding Entity 1 holds a 10% interest in the first entity, and Holding Entity 2 holds a 10% interest in Holding Entity 1, the information mentioned in paragraphs (1)(h) and (ha) relating to those holding entities, would be given to the Secretary.

Note 2: For the definition of ***influence or control***, see section 8A.

Note 3: For interests held by trusts, partnerships, superannuation funds and unincorporated foreign companies, see section 53A.

(2) Information under subsection (1) may include personal information (within the meaning of the *Privacy Act 1988*).

Authorised Version C2022C00160 registered 02/05/2022

Interest and control information provided by States and Territories

(3) If the first entity is a Governor, First Minister, Administrator or Minister of a State or Territory who is a direct interest holder in relation to an asset because of paragraph 8(1)(b), the first entity is not required to provide any interest and control information.

(4) However, subsection (3) does not affect the obligation of the State or Territory to provide interest and control information in relation to the asset if the State or Territory is also a direct interest holder in relation to the asset because of paragraph 8(1)(a) or (b).

Interest and control information provided by the Commonwealth

(5) If the first entity:
  (a) is the Governor-General, the Prime Minister or a Minister; and
  (b) is a direct interest holder in relation to an asset because of paragraph 8(1)(b);

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

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

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

7 Meaning of *operational information*

(1) The following information is ***operational information*** in relation to an asset:
  (a) the location of the asset;
  (b) a description of the area the asset services;
  (c) the following information about each entity that is the responsible entity for, or an operator of, the asset:
    (i) the name of the entity;

Authorised Version C2022C00160 registered 02/05/2022

(ii) if applicable, the ABN of the entity, or other similar business number (however described) if the entity was incorporated, formed or created (however described) outside Australia;

(iii) the address of the entity's head office or principal place of business;

(iv) the country in which the entity was incorporated, formed or created (however described);

(d) the following information about the chief executive officer (however described) of the responsible entity for the asset:

(i) the full name of the officer;

(ii) the country or countries of which the officer is a citizen;

(e) a description of the arrangements under which each operator operates the asset or a part of the asset;

(f) a description of the arrangements under which data prescribed by the rules relating to the asset is maintained;

(g) information prescribed by the rules for the purposes of this paragraph.

Note: For paragraph (e), this would include if the control system of the asset is managed by a separate body.

(2) Information under subsection (1) may include personal information (within the meaning of the *Privacy Act 1988*).

8 Meaning of *direct interest holder*

(1) An entity is a ***direct interest holder*** in relation to an asset if the entity:

(a) together with any associates of the entity, holds an interest of at least 10% in the asset (including if any of the interests are held jointly with one or more other entities); or

(b) holds an interest in the asset that puts the entity in a position to directly or indirectly influence or control the asset.

Note: For interests held by trusts, partnerships, superannuation funds and unincorporated foreign companies, see section 53A.

Authorised Version C2022C00160 registered 02/05/2022

Exemption for moneylenders etc.

(2) Subsection (1) does not apply to an interest in an asset held by an entity if:

(a) the entity holds the interest in the asset:

(i) solely by way of security for the purposes of a moneylending agreement; or

(ii) solely as a result of enforcing a security for the purposes of a moneylending agreement; and

(b) the entity is:

(i) the entity (the ***first entity***) that entered into the moneylending agreement; or

(ii) a subsidiary or holding entity of the first entity; or

(iii) a person who is (alone or with others) in a position to determine the investments or policy of the first entity; or

(iv) a security trustee who holds or acquires the interest on behalf of the first entity; or

(v) a receiver, or a receiver and manager, appointed by, or appointed on instructions from, a person or entity mentioned in any of subparagraphs (i) to (iv).

(3) A ***moneylending agreement*** is:

(a) an agreement entered into in good faith, on ordinary commercial terms and in the ordinary course of carrying on a business (a ***moneylending business***) of lending money or otherwise providing financial accommodation, except an agreement dealing with any matter unrelated to the carrying on of that business; or

(b) if the entity:

(i) is carrying on a moneylending business; or

(ii) is a subsidiary or holding entity of a corporate entity that is carrying on a moneylending business;

an agreement to acquire an interest arising from a moneylending agreement (within the meaning of paragraph (a)).

Authorised Version C2022C00160 registered 02/05/2022

Exemption for providers of custodial or depository services

(4) Subsection (1) does not apply to an interest in an asset held by an entity if:
  (a) the entity is the provider of a custodial or depository service; and
  (b) the entity holds the interest in the asset solely in the entity's capacity as the provider of a custodial or depository service; and
  (c) the holding of the interest does not put the entity in a position to directly or indirectly influence or control the asset.

Exemption for providers of services specified in the rules

(5) Subsection (1) does not apply to an interest in an asset held by an entity if:
  (a) the entity is the provider of a service specified in the rules; and
  (b) the entity holds the interest in the asset solely in the entity's capacity as the provider of the service; and
  (c) the holding of the interest does not put the entity in a position to directly or indirectly influence or control the asset.

8A Meaning of *influence or control*

(1) An entity is in a position to directly or indirectly ***influence or control*** an asset if:
  (a) the entity is in a position to exercise voting or veto rights in relation to the body that governs the asset; or
  (b) the entity is in a position to make decisions that materially impact on the running of, or strategic direction in relation to, the asset; or
  (c) the entity has the ability to appoint:
    (i) persons to the body that governs the asset; or
    (ii) key personnel involved in running the asset; or
  (d) the entity is in a position to influence or determine decisions relating to:

Authorised Version C2022C00160 registered 02/05/2022

(i) the business plan, or any other management plan, for the asset; or
(ii) major expenditure relating to the asset; or
(iii) major contracts or transactions involving the asset; or
(iv) major loans involving the asset.

Note: For interests held by trusts, partnerships, superannuation funds and unincorporated foreign companies, see section 53A.

(2) An entity (the ***controlling entity***) is in a position to directly or indirectly ***influence or control*** another entity (the ***controlled entity***) if the controlling entity:
(a) is in a position to exercise voting or veto rights in relation to the controlled entity; or
(b) is in a position to make decisions that materially impact on the running of, or strategic direction of, the controlled entity; or
(c) has the ability to appoint persons to the board of the controlled entity; or
(d) is in a position to influence or determine decisions relating to:
(i) the business plan, or any other management plan, for the controlled entity; or
(ii) major expenditure relating to the controlled entity; or
(iii) major contracts or transactions involving the controlled entity; or
(iv) major loans involving the controlled entity; or
(e) together with any associates of the controlling entity, holds an interest of at least 10% in the controlled entity (including if any of the interests are held jointly with one or more other entities).

(3) This section does not limit when an entity is in a position to directly or indirectly ***influence or control*** an asset or other entity.

8B Meaning of *associate*

Each of the following persons is an ***associate*** of a person:

Authorised Version C2022C00160 registered 02/05/2022

(a) any relative of the person;
(b) any person with whom the person is acting, or proposes to act, in concert in relation to an asset;
(c) any person with whom the person carries on a business in partnership;
(d) any corporate entity of which the person is a senior officer;
(e) if the person is a corporate entity:
  (i) any holding entity of the corporate entity; or
  (ii) any senior officer of the corporate entity;
(f) any corporate entity whose senior officers are accustomed or under an obligation (whether formal or informal) to act in accordance with the directions, instructions or wishes of:
  (i) the person; or
  (ii) if the person is a corporate entity—the senior officers of the person;
(g) a corporate entity if the person is accustomed or under an obligation (whether formal or informal) to act in accordance with the directions, instructions or wishes of:
  (i) the corporate entity; or
  (ii) the senior officers of the corporate entity;
(h) any body corporate in which the person holds an interest;
(i) if the person is a body corporate—a person who holds an interest in the body corporate;
(j) the trustee of a trust in which the person holds an interest;
(k) if the person is the trustee of a trust—a person who holds an interest in the trust;
(l) any other person or body prescribed by the rules.

8C Meanings of *subsidiary* and *holding entity*

Meaning of ***subsidiary***

(1) A corporate entity (the ***lower entity***) is a ***subsidiary*** of another corporate entity (the ***higher entity***) if:
  (a) the higher entity:

Authorised Version C2022C00160 registered 02/05/2022

(i) is in a position to control more than half the voting power in the lower entity; or

(ii) holds more than half the issued securities in the lower entity (disregarding any securities that carry no right to participate beyond a specified amount in a distribution of either profits or capital); or

(b) the lower entity is a subsidiary of a corporate entity that is the higher entity's subsidiary (including because of one or more applications of this subsection).

Meaning of ***holding entity***

(2) A corporate entity (the ***higher entity***) is a ***holding entity*** of another corporate entity (the ***lower entity***) if the lower entity is a subsidiary of the higher entity.

8D Meaning of *critical infrastructure sector*

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

(a) the communications sector;

(b) the data storage or processing sector;

(c) the financial services and markets sector;

(d) the water and sewerage sector;

(e) the energy sector;

(f) the health care and medical sector;

(g) the higher education and research sector;

(h) the food and grocery sector;

(i) the transport sector;

(j) the space technology sector;

(k) the defence industry sector.

8E Meaning of *critical infrastructure sector asset*

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

Authorised Version C2022C00160 registered 02/05/2022

Deeming—when asset relates to a sector

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

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

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

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

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

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

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

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

(10) For the purposes of this Act, each of the following assets is taken to relate to the transport sector:

Authorised Version C2022C00160 registered 02/05/2022

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

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

8F Critical infrastructure sector for a critical infrastructure asset

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

8G Meaning of *relevant impact*

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

(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.

9 Meaning of *critical infrastructure asset*

(1) An asset is a ***critical infrastructure asset*** if it is:
(a) a critical telecommunications asset; or
(b) a critical broadcasting asset; or
(c) a critical domain name system; or
(d) a critical data storage or processing asset; or
(da) a critical banking asset; or
(db) a critical superannuation asset; or
(dc) a critical insurance asset; or
(dd) a critical financial market infrastructure asset; or
(de) a critical water asset; or

Authorised Version C2022C00160 registered 02/05/2022

(df) a critical electricity asset; or
(dg) a critical gas asset; or
(dh) a critical energy market operator asset; or
(di) a critical liquid fuel asset; or
(dj) a critical hospital; or
(dk) a critical education asset; or
(dl) a critical food and grocery asset; or
(dm) a critical port; or
(dn) a critical freight infrastructure asset; or
(do) a critical freight services asset; or
(dp) a critical public transport asset; or
(dq) a critical aviation asset; or
(dr) a critical defence industry asset; or
(e) an asset declared under section 51 to be a critical infrastructure asset; or
(f) an asset prescribed by the rules for the purposes of this paragraph.

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

(2) However, the rules may prescribe that a specified:
(a) a critical telecommunications asset; or
(b) a critical broadcasting asset; or
(c) a critical domain name system; or
(d) a critical data storage or processing asset; or
(e) a critical banking asset; or
(f) a critical superannuation asset; or
(g) a critical insurance asset; or
(h) a critical financial market infrastructure asset; or
(i) a critical water asset; or
(j) a critical electricity asset; or
(k) a critical gas asset; or
(l) a critical energy market operator asset; or
(m) a critical liquid fuel asset; or

Authorised Version C2022C00160 registered 02/05/2022

(n) a critical hospital; or
(o) a critical education asset; or
(p) a critical food and grocery asset; or
(q) a critical port; or
(r) a critical freight infrastructure asset; or
(s) a critical freight services asset; or
(t) a critical public transport asset; or
(u) a critical aviation asset; or
(v) a critical defence industry asset;

is not a critical infrastructure asset.

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

(2A) If an asset is owned by:
(a) the Commonwealth; or
(b) a body corporate established by a law of the Commonwealth (other than a government business enterprise);

the asset is not a critical infrastructure asset unless:
(c) the asset is declared under section 51 to be a critical infrastructure asset; or
(d) the asset is prescribed by the rules for the purposes of paragraph (1)(f).

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

Prescribing an asset as a critical infrastructure asset

(3) The Minister must not prescribe an asset for the purposes of paragraph (1)(f) unless the Minister is satisfied that:
(a) the asset is critical to:
(i) the social or economic stability of Australia or its people; or
(ii) the defence of Australia; or
(iii) national security; and
(b) the asset relates to a critical infrastructure sector.

Authorised Version C2022C00160 registered 02/05/2022

Consultation with State and Territory Ministers

(4) The Minister (the ***Commonwealth Minister***) also must not prescribe the asset unless the Commonwealth Minister has:
  (a) consulted the following persons (the ***consulted Minister***):
    (i) the First Minister of the State, the Australian Capital Territory or the Northern Territory in which the critical infrastructure asset is wholly or partly located;
    (ii) each 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 in that State or Territory; and
  (b) given each consulted Minister written notice of the proposal to prescribe the asset; and
  (c) had regard to any representations given by a consulted Minister under subsection (5) within the period specified for that purpose.

(5) The notice must invite each consulted Minister to make written representations to the Commonwealth Minister in relation to the proposal to prescribe the asset within the period specified in the notice, which must be:
  (a) at least 28 days after the notice is given; or
  (b) a shorter period if the Commonwealth Minister considers the shorter period is necessary because of urgent circumstances.

(6) Subsection (4) does not limit the persons with whom the Commonwealth Minister may consult.

10 Meaning of *critical electricity asset*

(1) An asset is a ***critical electricity asset*** if it is:
  (a) a network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers or any other number of customers prescribed by the rules; or

Authorised Version C2022C00160 registered 02/05/2022

(b) an electricity generation station that is critical to ensuring the security and reliability of electricity networks or electricity systems in a State or Territory, in accordance with subsection (2).

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

(2) For the purposes of paragraph (1)(b), the rules may prescribe requirements for an electricity generation station to be critical to ensuring the security and reliability of electricity networks or electricity systems in a particular State or Territory.

11 Meaning of *critical port*

An asset is a ***critical port*** if it is land that forms part of any of the following security regulated ports:

(a) Broome Port;
(b) Port Adelaide;
(c) Port of Brisbane;
(d) Port of Cairns;
(e) Port of Christmas Island;
(f) Port of Dampier;
(g) Port of Darwin;
(h) Port of Eden;
(i) Port of Fremantle;
(j) Port of Geelong;
(k) Port of Gladstone;
(l) Port of Hay Point;
(m) Port of Hobart;
(n) Port of Melbourne;
(o) Port of Newcastle;
(p) Port of Port Botany;
(q) Port of Port Hedland;
(r) Port of Rockhampton;
(s) Port of Sydney Harbour;

Authorised Version C2022C00160 registered 02/05/2022

(t) Port of Townsville;

(u) a security regulated port prescribed by the rules for the purposes of this paragraph.

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

12 Meaning of *critical gas asset*

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

(a) a gas processing facility that has a capacity of at least 300 terajoules per day or any other capacity prescribed by the rules;

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

(c) a network or system for the distribution of gas to ultimately service at least 100,000 customers or any other number of customers prescribed by the rules;

(d) a gas transmission pipeline that is critical to ensuring the security and reliability of a gas market, in accordance with subsection (2);

(e) a control room, or any other asset, that is required to operate a gas transmission pipeline covered by paragraph (d).

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

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

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

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

12A Meaning of *critical liquid fuel asset*

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

Authorised Version C2022C00160 registered 02/05/2022

(a) a liquid fuel refinery that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (2);
(b) a liquid fuel pipeline that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (3);
(c) a liquid fuel storage facility that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (4).

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

(2) For the purposes of paragraph (1)(a), the rules may prescribe:
(a) specified liquid fuel refineries that are critical to ensuring the security and reliability of a liquid fuel market; or
(b) requirements for a liquid fuel refinery to be critical to ensuring the security and reliability of a liquid fuel market.

(3) For the purposes of paragraph (1)(b), the rules may prescribe:
(a) specified liquid fuel pipelines that are critical to ensuring the security and reliability of a liquid fuel market; or
(b) requirements for a liquid fuel pipeline to be critical to ensuring the security and reliability of a liquid fuel market.

(4) For the purposes of paragraph (1)(c), the rules may prescribe:
(a) specified liquid fuel storage facilities that are critical to ensuring the security and reliability of a liquid fuel market; or
(b) requirements for a liquid fuel storage facility to be critical to ensuring the security and reliability of a liquid fuel market.

12B Meaning of *critical freight infrastructure asset*

(1) An asset is a ***critical freight infrastructure asset*** if it is any of the following:
(a) a road network that, in accordance with subsection (2), functions as a critical corridor for the transportation of goods between:

Authorised Version C2022C00160 registered 02/05/2022

(i) 2 States; or
(ii) a State and a Territory; or
(iii) 2 Territories; or
(iv) 2 regional centres;

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

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

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

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

(a) specified road networks that function as a critical corridor for the transportation of goods between:
(i) 2 States; or
(ii) a State and a Territory; or
(iii) 2 Territories; or
(iv) 2 regional centres; or

(b) requirements for a road network to function as a critical corridor for the transportation of goods between:
(i) 2 States; or
(ii) a State and a Territory; or
(iii) 2 Territories; or
(iv) 2 regional centres.

Authorised Version C2022C00160 registered 02/05/2022

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

(4) For the purposes of paragraph (1)(c), the rules may prescribe:
  (a) specified intermodal transfer facilities that are critical to the transportation of goods between:
    (i) 2 States; or
    (ii) a State and a Territory; or
    (iii) 2 Territories; or
    (iv) 2 regional centres; or
  (b) requirements for an intermodal transfer facility to be critical to the transportation of goods between:
    (i) 2 States; or
    (ii) a State and a Territory; or
    (iii) 2 Territories; or
    (iv) 2 regional centres.

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

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

Authorised Version C2022C00160 registered 02/05/2022

12C Meaning of *critical freight services asset*

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

(a) road;

(b) rail;

(c) inland waters;

(d) sea.

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

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

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

(i) road;

(ii) rail;

(iii) inland waters;

(iv) sea; or

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

(i) road;

(ii) rail;

(iii) inland waters;

(iv) sea.

12D Meaning of *critical financial market infrastructure asset*

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

(a) an asset that:

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

(ii) is used in connection with the operation of a financial market that, in accordance with subsection (2), is critical

Authorised Version C2022C00160 registered 02/05/2022

to the security and reliability of the financial services and markets sector;

(b) an asset that:

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

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

(c) an asset that:

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

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

(d) an asset that:

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

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

(e) an asset that:

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

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

(f) an asset that:

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

Authorised Version C2022C00160 registered 02/05/2022

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

(g) an asset that:

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

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

(h) an asset that:

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

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

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

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

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

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

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

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

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

12E Meaning of *critical broadcasting asset*

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

(a) the broadcasting transmission assets are:

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

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

(b) the broadcasting transmission assets are:

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

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

(iii) not broadcasting re-transmission assets; or

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

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

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

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

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

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

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

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

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

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

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

(b) it is used wholly or primarily to provide a data storage or processing service that relates to business critical data and that is provided by the entity to an end-user that is:

Authorised Version C2022C00160 registered 02/05/2022

(i) the Commonwealth; or
(ii) a body corporate established by a law of the Commonwealth; or
(iii) a State; or
(iv) a body corporate established by a law of a State; or
(v) a Territory; or
(vi) a body corporate established by a law of a Territory; and

(c) the entity knows that the asset is used as described in paragraph (b); and
(d) the asset is not a critical infrastructure asset that is covered by a paragraph of subsection 9(1) (other than paragraph 9(1)(d)).

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

(2) An asset is a ***critical data storage or processing asset*** if:
(a) it is owned or operated by an entity that is a data storage or processing provider; and
(b) it is used wholly or primarily to provide a data storage or processing service that:
(i) is provided by the entity to an end-user that is the responsible entity for a critical infrastructure asset; and
(ii) relates to business critical data; and
(c) the entity knows that the asset is used as described in paragraph (b); and
(d) the asset is not a critical infrastructure asset that is covered by a paragraph of subsection 9(1) (other than paragraph 9(1)(d)).

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

(3) If:
(a) an entity (the ***first entity***) is the responsible entity for a critical infrastructure asset; and
(b) the first entity becomes aware that a data storage or processing service:
(i) is provided by another entity on a commercial basis to the first entity; and

Authorised Version C2022C00160 registered 02/05/2022

(ii) relates to business critical data;

the first entity must:

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

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

(ii) relates to business critical data; and

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

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

12G Meaning of *critical banking asset*

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

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

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

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

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

(2) For the purposes of subparagraph (1)(a)(ii), the rules may prescribe:
  (a) specified authorised deposit-taking institutions that are critical to the security and reliability of the financial services and markets sector; or
  (b) requirements for an authorised deposit-taking institution to be critical to the security and reliability of the financial services and markets sector.

(3) For the purposes of subparagraph (1)(b)(ii), the rules may prescribe:
  (a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or
  (b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector.

12H Meaning of *critical insurance asset*

(1) An asset is a ***critical insurance asset*** if it is any of the following assets:
  (a) an asset where the following conditions are satisfied:
    (i) the asset is owned or operated by an entity that carries on insurance business;
    (ii) the entity is an entity that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector;
    (iii) the asset is used in connection with the carrying on of insurance business;
  (b) an asset where the following conditions are satisfied:
    (i) the asset is owned or operated by a body corporate that is a related body corporate of an entity that carries on insurance business;

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

(ii) the body corporate is a body corporate that, in accordance with subsection (7), is critical to the security and reliability of the financial services and markets sector;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

(6) For the purposes of subparagraph (1)(e)(ii), the rules may prescribe:
  (a) specified entities that are critical to the security and reliability of the financial services and markets sector; or
  (b) requirements for an entity to be critical to the security and reliability of the financial services and markets sector.

(7) For the purposes of subparagraph (1)(f)(ii), the rules may prescribe:
  (a) specified bodies corporate that are critical to the security and reliability of the financial services and markets sector; or
  (b) requirements for a body corporate to be critical to the security and reliability of the financial services and markets sector.

12J Meaning of *critical superannuation asset*

(1) An asset is a ***critical superannuation asset*** if:
  (a) it is owned or operated by an RSE licensee that, in accordance with subsection (2), is critical to the security and reliability of the financial services and markets sector; and
  (b) it is used in connection with the operation of a superannuation fund.

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

(2) For the purposes of paragraph (1)(a), the rules may prescribe:
  (a) specified RSE licensees that are critical to the security and reliability of the financial services and markets sector; or
  (b) requirements for an RSE licensee to be critical to the security and reliability of the financial services and markets sector.

12K Meaning of *critical food and grocery asset*

(1) An asset is a ***critical food and grocery asset*** if it is a network that:
  (a) is used for the distribution or supply of:
    (i) essential food; or

Authorised Version C2022C00160 registered 02/05/2022

(ii) essential groceries; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12KA Meaning of *critical domain name system*

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

(2) For the purposes of paragraph (1)(a), the rules may prescribe:
  (a) specified entities that are critical to the administration of an Australian domain name system; or
  (b) requirements for an entity to be critical to the administration of an Australian domain name system.

(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.

12L Meaning of *responsible entity*

Critical telecommunications asset

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

Critical broadcasting asset

(2) The responsible entity for a critical broadcasting asset is:
  (a) the entity referred to in whichever of the following provisions is applicable:
    (i) subparagraph 12E(1)(a)(i);
    (ii) subparagraph 12E(1)(b)(i);
    (iii) paragraph 12E(1)(c); or

Authorised Version C2022C00160 registered 02/05/2022

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

Critical domain name system

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

Critical data storage or processing asset

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

Critical banking asset

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

Critical superannuation asset

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

Authorised Version C2022C00160 registered 02/05/2022

Critical insurance asset

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

Critical financial market infrastructure asset

(8) The responsible entity for a critical financial market infrastructure asset is:
  (a) if the asset is covered by paragraph 12D(1)(a)—the body corporate referred to in subparagraph 12D(1)(a)(i); or
  (b) if the asset is covered by paragraph 12D(1)(b)—the associated entity referred to in subparagraph 12D(1)(b)(i); or
  (c) if the asset is covered by paragraph 12D(1)(c)—the body corporate referred to in subparagraph 12D(1)(c)(i); or
  (d) if the asset is covered by paragraph 12D(1)(d)—the associated entity referred to in subparagraph 12D(1)(d)(i); or
  (e) if the asset is covered by paragraph 12D(1)(e)—the body corporate referred to in subparagraph 12D(1)(e)(i); or
  (f) if the asset is covered by paragraph 12D(1)(f)—the associated entity referred to in subparagraph 12D(1)(f)(i); or
  (g) if the asset is covered by paragraph 12D(1)(g)—the body corporate referred to in subparagraph 12D(1)(g)(i); or

Authorised Version C2022C00160 registered 02/05/2022

(h) if the asset is covered by paragraph 12D(1)(h)—the associated entity referred to in subparagraph 12D(1)(h)(i); or
(i) if the asset is covered by paragraph 12D(1)(i)—the entity prescribed by the rules; or
(j) if another entity is prescribed by the rules in relation to the asset—that other entity.

Critical water asset

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

Critical electricity asset

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

Critical gas asset

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

Critical energy market operator asset

(12) The responsible entity for a critical energy market operator asset is:

Authorised Version C2022C00160 registered 02/05/2022

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

Critical liquid fuel asset

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

Critical hospital

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

Authorised Version C2022C00160 registered 02/05/2022

Critical education asset

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

Critical food and grocery asset

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

Critical port

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

Critical freight infrastructure asset

(18) The responsible entity for a critical freight infrastructure asset is:
  (a) if the Commonwealth is responsible for the management of the asset—the Commonwealth; or
  (b) if a State is responsible for the management of the asset—the State; or
  (c) if a Territory is responsible for the management of the asset—the Territory; or
  (d) if a body is:
    (i) established by a law of the Commonwealth, a State or a Territory; and
    (ii) responsible for the management of the asset;

Authorised Version C2022C00160 registered 02/05/2022

that body; or

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

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

Critical freight services asset

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

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

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

Critical public transport asset

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

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

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

Critical aviation asset

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

(a) if the asset is:

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

(ii) owned or operated by an aircraft operator;

the aircraft operator; or

(b) if the asset is:

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

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

the regulated air cargo agent; or

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

Authorised Version C2022C00160 registered 02/05/2022

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

Critical defence industry asset

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

Assets prescribed by the rules

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

Assets declared to be a critical infrastructure asset

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

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.

12M Meaning of *cyber security incident*

A ***cyber security incident*** is one or more acts, events or circumstances involving any of the following:
(a) unauthorised access to:
(i) computer data; or
(ii) a computer program;
(b) unauthorised modification of:

Authorised Version C2022C00160 registered 02/05/2022

(i) computer data; or
(ii) a computer program;

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

(d) unauthorised impairment of the availability, reliability, security or operation of:
(i) a computer; or
(ii) computer data; or
(iii) a computer program.

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

(1) For the purposes of this Act:

(a) access to:
(i) computer data; or
(ii) a computer program; or

(b) modification of:
(i) computer data; or
(ii) a computer program; or

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

(d) the impairment of the availability, reliability, security or operation of:
(i) a computer; or
(ii) computer data; or
(iii) a computer program;

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

(3) For the purposes of subsection (1), if:
  (a) a person causes any access, modification or impairment of a kind mentioned in that subsection; and
  (b) the person does so:
    (i) under a warrant issued under a law of the Commonwealth, a State or a Territory; or
    (ii) under an emergency authorisation given to the person under Part 3 of the *Surveillance Devices Act 2004* or under a law of a State or Territory that makes provision to similar effect; or
    (iii) under a tracking device authorisation given to the person under section 39 of the *Surveillance Devices Act 2004*; or
    (iv) in accordance with a technical assistance request; or
    (v) in compliance with a technical assistance notice; or
    (vi) in compliance with a technical capability notice;

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

12P Examples of responding to a cyber security incident

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

Authorised Version C2022C00160 registered 02/05/2022

Division 3—Constitutional provisions and application of this Act

13 Application of this Act

(1) This Act applies to the following:

(a) an entity that is a corporation to which paragraph 51(xx) of the Constitution applies;

(b) an entity, so far as the entity is the responsible entity for, a reporting entity for, a relevant entity for, or an operator of, an asset that is:

(i) in a Territory; or

(ii) used in the course of, or in relation to, trade or commerce with other countries, among the States, between Territories or between a Territory and a State; or

(iii) used for the purposes of the defence of Australia; or

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

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

(vi) used to supply a carriage service; or

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

(viii) used to administer a domain name system;

(c) an entity that is an alien (within the meaning of paragraph 51(xix) of the Constitution).

(2) Division 3 of Part 4 (use and disclosure of protected information) and section 60AA (acquisition of property) also apply to any other entity.

Note: For the definition of ***entity***, see section 5.

Authorised Version C2022C00160 registered 02/05/2022

14 Extraterritoriality

This Act applies both within and outside Australia.

Note: This Act extends to every external Territory.

15 This Act binds the Crown

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

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

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

16 Concurrent operation of State and Territory laws

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

17 State constitutional powers

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

Authorised Version C2022C00160 registered 02/05/2022

Part 2—Register of Critical Infrastructure Assets

Division 1—Introduction

18 Simplified outline of this Part

The Secretary must keep a Register of Critical Infrastructure Assets, containing information in relation to those assets. The Register must not be made public.

The responsible entity for a critical infrastructure asset must give the Secretary operational information in relation to the asset.

An entity that is a direct interest holder in relation to a critical infrastructure asset must give the Secretary interest and control information in relation to the entity and the asset.

If particular events occur in relation to the asset, the relevant reporting entity for the asset must notify the Secretary of the event and provide certain information.

If an entity required to give notice or information dies or is wound up before doing so, the entity's executor or liquidator must give the notice or information. An agent may give notice or information for an entity.

The rules may provide for exemptions from these requirements.

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

18A Application of this Part

(1) This Part applies to a critical infrastructure asset if:
  (a) the asset is specified in the rules; or
  (b) both:

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

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

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

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

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

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

18AA Consultation—rules

Scope

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

Consultation

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

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

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

(ii) inviting persons to make submissions to the Minister about the draft rules or amendments within the period specified in the notice; and

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

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

(3) The period specified in the notice must not be shorter than 28 days.

Authorised Version C2022C00160 registered 02/05/2022

Division 2—Register of Critical Infrastructure Assets

19 Secretary must keep Register

The Secretary must keep a Register of Critical Infrastructure Assets, containing:

(a) the information obtained by the Secretary under Division 3 (obligation to give information and notify of events); and

(b) any information added under section 20; and

(c) any corrections or updates of information described in paragraph (a) or (b) that are made under section 21.

20 Secretary may add information to Register

The Secretary may add to the Register any of the following that is obtained by the Secretary (other than information obtained under Division 3):

(a) operational information in relation to a critical infrastructure asset;

(b) interest and control information in relation to a direct interest holder and a critical infrastructure asset.

21 Secretary may correct or update information in the Register

The Secretary may correct or update information in the Register.

22 Register not to be made public

The Secretary must ensure that the Register is not made public.

Note: See Division 3 of Part 4 for the recording, use and disclosure of protected information that may be contained in the Register.

Authorised Version C2022C00160 registered 02/05/2022

Division 3—Obligation to give information and notify of events

23 Initial obligation to give information

(1) This section applies if an entity is, or will be, a reporting entity for a critical infrastructure asset at the end of the grace period for the asset.

Note: Once an entity has given information in relation to an asset under this section, the reporting entity for the asset must comply with section 24 (ongoing obligation to give information and notify of events).

(2) The entity must give the Secretary the following information in accordance with subsection (3):

(a) if the reporting entity is the responsible entity for the asset—the operational information in relation to the asset;

(b) if the reporting entity is a direct interest holder in relation to the asset—the interest and control information in relation to the entity and the asset.

Note 1: Persons other than the entity may give the information (see section 30 (agents may give notice or information) and Division 2 of Part 7 (treatment of certain entities)).

Note 2: For an exception to this section, see section 25 (information that is not able to be obtained).

Civil penalty: 50 penalty units.

(3) The information must be given:

(a) in the approved form; and

(b) by the later of:

(i) the end of the grace period for the asset; and

(ii) the end of 30 days after the day the entity becomes a reporting entity for the asset.

Authorised Version C2022C00160 registered 02/05/2022

24 Ongoing obligation to give information and notify of events

(1) This section applies to a reporting entity for a critical infrastructure asset if a notifiable event occurs in relation to the asset:
  (a) after the entity gives information in relation to the asset under section 23; or
  (b) after the end of the grace period for the asset.

Requirement to give information and notify of events

(2) If the reporting entity is required to give information in relation to the event in accordance with subsection (3), the reporting entity for the asset must give the Secretary that information and notice of the event:
  (a) in the approved form; and
  (b) by the end of 30 days after the event occurs.

Note 1: Persons other than the entity may give the information (see section 30 (agents may give notice or information) and Division 2 of Part 7 (treatment of certain entities)).

Note 2: For an exception to this section, see section 25 (information that is not able to be obtained).

Civil penalty: 50 penalty units.

(3) The following table sets out the information a reporting entity is required to give in relation to the event.

Ongoing obligation to give information			
Item	**If the event is ...**	**this reporting entity ...**	**must give this information ...**
1	an event covered by subparagraph 26(a)(i)	the entity that is the responsible entity for the asset immediately after the event occurs	any operational information in relation to the asset that is necessary to correct or complete the operational information, in relation to the asset, previously

Authorised Version C2022C00160 registered 02/05/2022

Ongoing obligation to give information			
Item	**If the event is ...**	**this reporting entity ...**	**must give this information ...**
			obtained by the Secretary.
2	an event covered by subparagraph 26(a)(ii)	the entity that is the direct interest holder to which the information relates	any interest and control information in relation to the entity and the asset that is necessary to correct or complete the interest and control information, in relation to the entity and the asset, previously obtained by the Secretary.
3	an event covered by paragraph 26(b) or (c) relating to the responsible entity for the asset	the responsible entity for the asset	the operational information in relation to the asset.
4	an event covered by paragraph 26(b) or (c) relating to a direct interest holder in relation to the asset	the direct interest holder in relation to the asset	the interest and control information in relation to the entity and the asset.

Exception to requirement to give information

(4) However, subsection (2) does not apply in relation to the event (the ***first event***) if:

(a) before the end of 30 days after the first event occurs, another notifiable event (the ***second event***) occurs in relation to the asset; and

(b) a result of the second event is that the information in relation to the asset that was required to be given to the Secretary

Authorised Version C2022C00160 registered 02/05/2022

under subsection (2) following the first event is no longer correct.

Note: An entity that wishes to rely on subsection (4) in proceedings for a civil penalty order bears an evidential burden in relation to the matter in that subsection (see section 96 of the Regulatory Powers Act).

25 Information that is not able to be obtained

Section 23 (initial obligation to give information) or 24 (ongoing obligation to give information and notify of events) does not apply in relation to particular information that a person is required to provide under that section if:

(a) the person uses the person's best endeavours to obtain the information; and

(b) the person is not able to obtain the information.

Note: An entity that wishes to rely on this section in proceedings for a civil penalty order bears an evidential burden in relation to the matter in that subsection (see section 96 of the Regulatory Powers Act).

26 Meaning of *notifiable event*

An event is a ***notifiable event*** in relation to a critical infrastructure asset if:

(a) the event has the effect that either of the following previously obtained by the Secretary for the purposes of this Act becomes incorrect or incomplete:

(i) the operational information in relation to the asset;

(ii) the interest and control information in relation to a direct interest holder and the asset; or

(b) the event is an entity becoming a reporting entity for the asset; or

(c) the event is a reporting entity for the asset becoming an entity to which this Act applies (see section 13).

Note: If an asset becomes a critical infrastructure asset after the end of the period of 6 months starting on the commencing day, a reporting entity for the asset initially has a period of between 30 days and 6 months in which to provide information in relation to the asset (see section 23).

Authorised Version C2022C00160 registered 02/05/2022

27 Rules may exempt from requirement to give notice or information

The rules may provide that this Division, or specified provisions of this Division, do not apply in relation to:

(a) any entity; or

(b) specified classes of entities; or

(c) specified entities;

either generally or in specified circumstances.

Note: An entity that wishes to rely on an exemption in the rules in relation to a contravention of section 23 or 24 bears an evidential burden (see section 96 of the Regulatory Powers Act).

Authorised Version C2022C00160 registered 02/05/2022

Division 4—Giving of notice or information by agents etc.

28 Requirement for executors and administrators to give notice or information for individuals who die

If an individual, who is required by section 23 or 24 to give notice or information, dies before giving the notice or information, the executor or administrator of the individual's estate must give the notice or information in accordance with that section.

29 Requirement for corporate liquidators etc. to give notice or information

If an entity that is required by section 23 or 24 to give notice or information is a corporation that:

(a) is placed into voluntary administration, liquidation or receivership before giving the notice or information; and

(b) is no longer in a position to give the notice or information;

the voluntary administrator, liquidator or receiver of the corporation must give the notice or information in accordance with that section.

30 Agents may give notice or information

An entity required by section 23 or 24 to give notice or information is taken to have complied with the requirement if someone else gives the notice or information, in accordance with that section, on the entity's behalf.

Authorised Version C2022C00160 registered 02/05/2022

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 (unless an exemption applies).
- 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:

Authorised Version C2022C00160 registered 02/05/2022

(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 subsections (3), (4), (5) and (6).

Exemptions

(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.

(4) If:

(a) an entity holds a certificate of hosting certification (strategic level) that relates to one or more services; and

(b) the certificate was issued under the scheme that is:

(i) administered by the Commonwealth; and

(ii) known as the hosting certification framework; and

(c) a critical infrastructure asset, or a part of a critical infrastructure asset, is used in connection with the provision of any of those services; and

(d) the entity is the responsible entity for the asset;

this Part does not apply to the asset.

Note: For reporting obligations, see Part 2AA.

(5) If:

(a) an entity is covered by a provision of a law of the Commonwealth, a State or a Territory; and

(b) the provision is specified in the rules; and

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

Authorised Version C2022C00160 registered 02/05/2022

this Part does not apply to the asset.

Note: For reporting obligations, see Part 2AA.

(6) If:

(a) a critical infrastructure asset is covered by a provision of a law of the Commonwealth, a State or a Territory; and

(b) the provision is specified in the rules;

this Part does not apply to the asset.

Note: For reporting obligations, see Part 2AA.

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 the period specified in the notice; and

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

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

(3) The period specified in the notice must not be shorter than 28 days.

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

Authorised Version C2022C00160 registered 02/05/2022

(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

Authorised Version C2022C00160 registered 02/05/2022

(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:

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

(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:
  (a) permit a background check of an individual to be conducted under the AusCheck scheme; and
  (b) provide that such a background check must include assessment of information relating to one or more of the matters mentioned in paragraphs 5(a), (b), (c) and (d) of the *AusCheck Act 2007*, as specified in the rules; and
  (c) provide that, if such a background check includes an assessment of information relating to the matter mentioned in paragraph 5(a) of the *AusCheck Act 2007*, the criteria against which that information must be assessed are the criteria specified in the rules; and
  (d) provide that, if such a background check includes assessment of information relating to the matter mentioned in paragraph 5(d) of the *AusCheck Act 2007*, the assessment must consist of whichever of the following is specified in the rules:
    (i) an electronic identity verification check;
    (ii) an in person identity verification check;
    (iii) both an electronic identity verification check and an in person identity verification check.

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

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

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.

30AKA Responsible entity must have regard to certain matters in deciding whether to adopt or vary critical infrastructure risk management program etc.

Adoption of program

(1) If an entity is the responsible entity for one or more critical infrastructure assets, then, in deciding whether to adopt a critical infrastructure risk management program, the entity must have regard to such matters (if any) as are set out in the rules.

Civil penalty: 200 penalty units.

Authorised Version C2022C00160 registered 02/05/2022

(2) Subsection (1) does not limit the matters to which the responsible entity may have regard.

Review of program

(3) 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;

then, in reviewing the program in accordance with section 30AE, the entity must have regard to such matters (if any) as are set out in the rules.

Civil penalty: 200 penalty units.

(4) Subsection (3) does not limit the matters to which the responsible entity may have regard.

Variation of program

(5) 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;

then, in deciding whether to vary the program, the entity must have regard to such matters (if any) as are set out in the rules.

Civil penalty: 200 penalty units.

(6) Subsection (5) does not limit the matters to which the responsible entity may have regard.

Rules

(7) Rules made for the purposes of subsection (1), (3) or (5):
  (a) may be of general application; or

Authorised Version C2022C00160 registered 02/05/2022

(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*.

(8) Subsection (7) of this section does not, by implication, limit subsection 33(3A) of the *Acts Interpretation Act 1901*.

30AL Consultation—rules made for the purposes of section 30AH or 30AKA

Scope

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

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 the period specified in the notice; and
  (b) give a copy of the notice to each First Minister; and
  (c) consider any submissions received within the period mentioned in paragraph (a).

(3) The period specified in the notice must not be shorter than 28 days.

(4) 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).

Authorised Version C2022C00160 registered 02/05/2022

30AM Review of rules

Scope

(1) This section applies if, because of subsection 30AL(4), 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 the period specified in the notice; and
  (b) give a copy of the notice to each First Minister; and
  (c) consider any submissions received within the period mentioned in paragraph (a).

(4) The period specified in the notice must not be shorter than 28 days.

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

Authorised Version C2022C00160 registered 02/05/2022

Minister to table statement of findings

(6) 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 or 30AKA.

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*.

30ANA Application, adoption or incorporation of certain documents

Application, adoption or incorporation of a relevant document

(1) Despite subsection 14(2) of the *Legislation Act 2003*, rules made for the purposes of section 30AH or 30AKA of this Act may make

Authorised Version C2022C00160 registered 02/05/2022

provision in relation to a matter by applying, adopting or incorporating, with or without modification, any matter contained in a relevant document as in force or existing from time to time.

Relevant document

(2) For the purposes of this section, ***relevant document*** means:
  (a) the document titled *Essential Eight Maturity Model* and published by the Australian Signals Directorate; or
  (b) the document titled *Framework for Improving Critical Infrastructure Cybersecurity* and published by the National Institute of Standards and Technology of the United States of America; or
  (c) the document titled *Cybersecurity Capability Maturity Model* and published by the Department of Energy of the United States of America; or
  (d) the document titled *The 2020-21 AESCSF Framework Core* and published by Australian Energy Market Operator Limited (ACN 072 010 327); or
  (e) the document titled *Cyber Supply Chain Risk Management* and published by the Australian Signals Directorate; or
  (f) a document specified in the rules.

(3) Subsection 13(3) of the *Legislation Act 2003* does not apply to paragraph (2)(f) of this section.

30ANB Consultation—rules made for the purposes of paragraph 30ANA(2)(f)

Scope

(1) This section applies to rules made for the purposes of paragraph 30ANA(2)(f).

Consultation

(2) Before making or amending the rules, the Minister must:
  (a) cause to be published on the Department's website a notice:

Authorised Version C2022C00160 registered 02/05/2022

(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 the period specified in the notice; and

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

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

(3) The period specified in the notice must not be shorter than 28 days.

30ANC Disallowance of rules

Scope

(1) This section applies to rules made for the purposes of paragraph 30ANA(2)(f).

Disallowance

(2) Either House of the Parliament may, following a motion upon notice, pass a resolution disallowing the rules. For the resolution to be effective:

(a) the notice must be given in that House within 15 sitting days of that House after the copy of the rules was tabled in that House under section 38 of the *Legislation Act 2003*; and

(b) the resolution must be passed, in pursuance of the motion, within 15 sitting days of that House after the giving of that notice.

(3) If neither House passes such a resolution, the rules take effect on the day immediately after the last day upon which such a resolution could have been passed if it were assumed that notice of a motion to disallow the rules was given in each House on the last day of the 15 sitting day period of that House mentioned in paragraph (2)(a).

(4) If:

(a) notice of a motion to disallow the rules is given in a House of the Parliament within 15 sitting days of that House after the

Authorised Version C2022C00160 registered 02/05/2022

copy of the rules was tabled in that House under section 38 of the *Legislation Act 2003*; and

(b) at the end of 15 sitting days of that House after the giving of that notice of motion:

(i) the notice has not been withdrawn and the motion has not been called on; or

(ii) the motion has been called on, moved and (where relevant) seconded and has not been withdrawn or otherwise disposed of;

the rules are then taken to have been disallowed, and subsection (3) does not apply to the rules.

(5) Section 42 (disallowance) of the *Legislation Act 2003* does not apply to the rules.

Note 1: The 15 sitting day notice period mentioned in paragraph (2)(a) of this section is the same as the 15 sitting day notice period mentioned in paragraph 42(1)(a) of the *Legislation Act 2003*.

Note 2: The 15 sitting day disallowance period mentioned in paragraph (2)(b) of this section is the same as the 15 sitting day disallowance period mentioned in paragraph 42(1)(b) of the *Legislation Act 2003*.

Authorised Version C2022C00160 registered 02/05/2022

Part 2AA—Reporting obligations relating to certain assets that are not covered by a critical infrastructure risk management program

30AP Simplified outline of this Part

- A responsible entity must give an annual report relating to certain assets that are not covered by a 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.

30AQ Reporting obligations relating to certain assets that are not covered by a critical infrastructure risk management program

Scope

(1) This section applies if, during a period (the ***relevant period***) that consists of the whole or a part of a financial year, an entity was the responsible entity for one or more critical infrastructure assets that are covered by subsection 30AB(4), (5) or (6).

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:

Authorised Version C2022C00160 registered 02/05/2022

(c) sets out the reason why those assets are covered by subsection 30AB(4), (5) or (6); 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 action (if any) taken by the entity for the purposes of mitigating the significant relevant impact of the hazard on the assets concerned; 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.

Authorised Version C2022C00160 registered 02/05/2022

Part 2B—Notification of cyber security incidents

30BA Simplified outline of this Part

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

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

30BB Application of this Part

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

30BBA Consultation—rules

Scope

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

Consultation

(2) Before making or amending the rules, the Minister must:
  (a) cause to be published on the Department's website a notice:
    (i) setting out the draft rules or amendments; and
    (ii) inviting persons to make submissions to the Minister about the draft rules or amendments within the period specified in the notice; and
  (b) give a copy of the notice to each First Minister; and
  (c) consider any submissions received within the period mentioned in paragraph (a); and
  (d) if the Minister is aware that an entity is the responsible entity for an asset that is, or is proposed to be, specified in the rules:
    (i) give the entity a copy of the draft rules or amendments; and
    (ii) if a submission is received from the entity within the period mentioned in paragraph (a)—give the entity a written statement that sets out the Minister's response to the submission.

(3) The period specified in the notice must not be shorter than 28 days.

30BC Notification of critical cyber security incidents

(1) If:
  (a) an entity is the responsible entity for a critical infrastructure asset; and
  (b) the entity becomes aware that:
    (i) a cyber security incident has occurred or is occurring; and

Authorised Version C2022C00160 registered 02/05/2022

(ii) the incident has had, or is having, a significant impact (whether direct or indirect) on the availability of the asset;

the entity must:

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

(i) is about the incident; and

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

(d) do so as soon as practicable, and in any event within 12 hours, after the entity becomes so aware.

Civil penalty: 50 penalty units.

Form of report etc.

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

(a) orally; or

(b) in writing.

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

(a) do both of the following:

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

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

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

Civil penalty: 50 penalty units.

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

Civil penalty: 50 penalty units.

Authorised Version C2022C00160 registered 02/05/2022

Exemption—written record

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

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

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

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

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

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

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

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

30BD Notification of other cyber security incidents

(1) If:

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

(b) the entity becomes aware that:

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

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

the entity must:

Authorised Version C2022C00160 registered 02/05/2022

(c) give the relevant Commonwealth body (see section 30BF) a report that:
  (i) is about the incident; and
  (ii) includes such information (if any) as is prescribed by the rules; and
(d) do so as soon as practicable, and in any event within 72 hours, after the entity becomes so aware.

Civil penalty: 50 penalty units.

Form of report etc.

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

(3) If a report under subsection (1) is given orally, the entity must:
  (a) do both of the following:
    (i) make a written record of the report in the approved form;
    (ii) give a copy of the written record of the report to the relevant Commonwealth body (see section 30BF); and
  (b) do so within 48 hours after the report is given.

Civil penalty: 50 penalty units.

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

Civil penalty: 50 penalty units.

Exemption—written record

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

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

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

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

30BE Liability

(1) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with section 30BC or section 30BD.

(2) An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1).

(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

Authorised Version C2022C00160 registered 02/05/2022

(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.

30BEA Significant impact

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

(a) both:

(i) the asset is used in connection with the provision of essential goods or services; and

(ii) the incident has materially disrupted the availability of those essential goods or services; or

(b) any of the circumstances specified in the rules exist in relation to the incident.

Authorised Version C2022C00160 registered 02/05/2022

30BEB Consultation—rules

Scope

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

Consultation

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

(3) The period specified in the notice must not be shorter than 28 days.

30BF Relevant Commonwealth body

For the purposes of this Part, ***relevant Commonwealth body*** means:
  (a) a Department that is specified in the rules; or
  (b) a body that is:
    (i) established by a law of the Commonwealth; and
    (ii) specified in the rules; or
  (c) if:
    (i) no rules are in force for the purposes of paragraph (a); and
    (ii) no rules are in force for the purposes of paragraph (b);

Authorised Version C2022C00160 registered 02/05/2022

ASD.

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

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) In deciding whether to give a notice to an entity under this section in relation to a system of national significance, the Secretary must have regard to:
  (a) the costs that are likely to be incurred by the entity in complying with Subdivision B; and
  (b) the reasonableness and proportionality of applying the statutory incident response planning obligations to the entity in relation to:
    (i) the system; and
    (ii) cyber security incidents; and
  (c) such other matters (if any) as the Secretary considers relevant.

(5) Before giving a notice to an entity under this section in relation to a system of national significance, the Secretary must consult:

Authorised Version C2022C00160 registered 02/05/2022

(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.

(6) 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

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

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;

Authorised Version C2022C00160 registered 02/05/2022

(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) In deciding whether to give a notice to an entity under subsection (1) or (2), 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) the reasonableness and proportionality of the requirement in the notice; and

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

(6) 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:

Authorised Version C2022C00160 registered 02/05/2022

(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*.

Authorised Version C2022C00160 registered 02/05/2022

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;

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

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:

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

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) In deciding whether to give a notice to an entity under subsection (1) or (2), 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) the reasonableness and proportionality of the requirement in the notice; and
  (c) such other matters (if any) as the Secretary considers relevant.

(4) 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

Authorised Version C2022C00160 registered 02/05/2022

(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:

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

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;

Authorised Version C2022C00160 registered 02/05/2022

(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

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

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

Authorised Version C2022C00160 registered 02/05/2022

(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) the reasonableness and proportionality of the requirements in the notice; and

(c) 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

Authorised Version C2022C00160 registered 02/05/2022

(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) the reasonableness and proportionality of the requirements in the notice; and
  (c) such other matters (if any) as the Secretary considers relevant.

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

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*).

Authorised Version C2022C00160 registered 02/05/2022

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) the reasonableness and proportionality of the requirements in the notice; and
  (c) 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

Authorised Version C2022C00160 registered 02/05/2022

(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:

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

Part 3—Directions by the Minister

Division 1—Simplified outline of this Part

31 Simplified outline of this Part

The Minister may require a reporting entity for, or an operator of, a critical infrastructure asset to do, or refrain from doing, an act or thing, if the Minister is satisfied that there is a risk of an act or omission that would be prejudicial to security.

The Minister may give the direction only if particular criteria are met and certain consultation has been undertaken.

Authorised Version C2022C00160 registered 02/05/2022

Division 2—Directions by the Minister

32 Direction if risk of act or omission that would be prejudicial to security

(1) This section applies if in connection with the operation of, or the delivery of a service by, a critical infrastructure asset the Minister is satisfied that there is a risk of an act or omission that would be prejudicial to security.

Direction to do, or refrain from doing, an act or thing

(2) The Minister may, subject to subsections (3) and (4), give an entity that is a reporting entity for, or an operator of, a critical infrastructure asset a written direction requiring the entity to do, or refrain from doing, a specified act or thing within the period specified in the direction.

(3) The Minister must not give the direction unless:

(a) the Minister is satisfied that requiring the entity to do, or to refrain from doing, the specified act or thing is reasonably necessary for purposes relating to eliminating or reducing the risk mentioned in subsection (1); and

(b) the Minister is satisfied that reasonable steps have been taken to negotiate in good faith with the entity to achieve an outcome of eliminating or reducing the risk without a direction being given under subsection (2); and

(c) an adverse security assessment in respect of the entity has been given to the Minister for the purposes of this section; and

(d) the Minister is satisfied that no existing regulatory system of the Commonwealth, a State or a Territory could instead be used to eliminate or reduce the risk mentioned in subsection (1).

Note: The Minister must also undertake consultation before giving a direction (see section 33).

Authorised Version C2022C00160 registered 02/05/2022

(3A) For the purposes of paragraph (3)(d), Division 3 of Part 3 of the *Foreign Acquisitions and Takeovers Act 1975* is to be ignored.

Matters etc. to which regard must be had

(4) Before giving the entity the direction, the Minister must have regard to the following:
  (a) the adverse security assessment mentioned in paragraph (3)(c);
  (b) the costs that would be likely to be incurred by the entity in complying with the direction;
  (c) the potential consequences that the direction may have on competition in the relevant critical infrastructure sector;
  (d) the potential consequences that the direction may have on customers of, or services provided by, the entity;
  (e) any representations given by the entity or a consulted Minister under subsection 33(2) within the period specified for that purpose.

(5) The Minister:
  (a) must give the greatest weight to the matter mentioned in paragraph (4)(a); and
  (b) may also have regard to any other matter the Minister considers relevant.

Other powers not limited

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

33 Consultation before giving direction

Consultation with relevant State or Territory Ministers

(1) Before giving an entity a direction under subsection 32(2), the Minister (the ***Commonwealth Minister***) must:
  (a) consult the following persons (the ***consulted Minister***):

Authorised Version C2022C00160 registered 02/05/2022

(i) the First Minister of the State, the Australian Capital Territory or the Northern Territory in which the critical infrastructure asset is wholly or partly located;

(ii) each Minister of the State, the Australian Capital Territory, or the Northern Territory, who has responsibility for the regulation or oversight of the relevant critical infrastructure sector in that State or Territory; and

(b) after reasonable steps have been taken to negotiate in good faith with the entity as described in paragraph 32(3)(b), give the entity and each consulted Minister written notice of the proposed direction.

(2) The notice must invite the entity and each consulted Minister to make written representations to the Commonwealth Minister in relation to the proposed direction within the period specified in the notice, which must be:

(a) at least 28 days after the notice is given; or

(b) a shorter period if the Commonwealth Minister considers the shorter period is necessary because of urgent circumstances.

(3) Subsection (1) does not limit the persons with whom the Commonwealth Minister may consult.

34 Requirement to comply with direction

An entity must comply with a direction given to the entity under subsection 32(2).

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

Civil penalty: 250 penalty units.

35 Exception—acquisition of property

Section 34 does not apply to the extent (if any) that its operation would result in an acquisition of property from a person otherwise than on just terms.

Authorised Version C2022C00160 registered 02/05/2022

Note: An entity that wishes to rely on this section in proceedings for a civil penalty order bears an evidential burden in relation to the matter in this section (see section 96 of the Regulatory Powers Act).

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).

35AAB Liability

(1) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with a direction under subsection 32(2).

(2) An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1) of this section.

(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:

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

Part 3A—Responding to serious cyber security incidents

Division 1—Simplified outline of this Part

35AA Simplified outline of this Part

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

Authorised Version C2022C00160 registered 02/05/2022

Division 2—Ministerial authorisation relating to cyber security incident

35AB Ministerial authorisation

Scope

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

(1A) This section also applies if the Minister is satisfied that:
  (a) a cyber security incident:
    (i) has occurred; or
    (ii) is occurring; or
    (iii) is imminent; and
  (b) the incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset (the ***primary asset***); and

Authorised Version C2022C00160 registered 02/05/2022

(c) the incident relates to an emergency specified in a national emergency declaration (within the meaning of the *National Emergency Declaration Act 2020*) that is in force; and

(d) no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident.

Authorisation

(2) The Minister may, on application by the Secretary, do any or all of the following things:

(a) authorise the Secretary to give directions to a specified entity under section 35AK that relate to the incident and the primary asset;

(b) authorise the Secretary to give directions to a specified entity under section 35AK that relate to the incident and a specified critical infrastructure sector asset;

(c) authorise the Secretary to give to a specified entity a specified direction under section 35AQ that relates to the incident and the primary asset;

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

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

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

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

Note 2: Section 35AQ deals with action directions.

Note 3: Section 35AX deals with intervention requests.

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

Information gathering directions

(5) A Ministerial authorisation under paragraph (2)(a) or (b):
  (a) is generally applicable to the incident and the asset concerned; and
  (b) is to be made without reference to any specific directions.

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

Action directions

(7) The Minister must not give a Ministerial authorisation under paragraph (2)(c) or (d) unless the Minister is satisfied that:
  (a) the specified entity is unwilling or unable to take all reasonable steps to respond to the incident; and
  (b) the specified direction is reasonably necessary for the purposes of responding to the incident; and
  (c) the specified direction is a proportionate response to the incident; and
  (d) compliance with the specified direction is technically feasible.

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

(8) In determining whether the specified direction is a proportionate response to the incident, the Minister must have regard to:
  (a) the impact of the specified direction on:
    (i) the activities carried on by the specified entity; and
    (ii) the functioning of the asset concerned; and

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

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

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

Intervention requests

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

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

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

(c) if there are 2 or more relevant entities for the asset concerned—those entities, when considered together, are unwilling or unable to take all reasonable steps to respond to the incident; and

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

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

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

(14) An agreement under subsection (13) may be given:
  (a) orally; or
  (b) in writing.

(15) If an agreement under subsection (13) is given orally, the Prime Minister or the Defence Minister, as the case requires, must:
  (a) do both of the following:
    (i) make a written record of the agreement;
    (ii) give a copy of the written record of the agreement to the Minister; and
  (b) do so within 48 hours after the agreement is given.

Ministerial authorisation is not a legislative instrument

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

Authorised Version C2022C00160 registered 02/05/2022

Other powers not limited

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

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

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

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

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

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

(d) access, add, restore, copy, alter or delete data held in:
  (i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or
  (ii) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

Authorised Version C2022C00160 registered 02/05/2022

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

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

(g) alter the functioning of:

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

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

(h) remove or disconnect:

(i) a computer; or

(ii) a computer device;

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

(i) connect or add:

(i) a computer; or

(ii) a computer device;

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

(j) remove:

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

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

from premises.

35AD Consultation

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

Authorised Version C2022C00160 registered 02/05/2022

(2) Before giving a Ministerial authorisation under paragraph 35AB(2)(e) or (f) in relation to an asset, the Minister must:
  (a) if the asset is a critical infrastructure asset—consult the responsible entity for the asset; or
  (b) if the asset is a critical infrastructure sector asset (other than a critical infrastructure asset)—consult whichever of the following entities the Minister considers to be most relevant in relation to the proposed authorisation:
    (i) the owner, or each of the owners, of the asset;
    (ii) the operator, or each of the operators, of the asset;

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

(3) If subsection (1) or (2) requires an entity to be consulted, that consultation must involve:
  (a) giving the entity a copy of the draft Ministerial authorisation; and
  (b) inviting the entity to make a submission to the Minister about the draft Ministerial authorisation within 24 hours after receiving the copy of the draft Ministerial authorisation.

35AE Form and notification of Ministerial authorisation

(1) A Ministerial authorisation may be given:
  (a) orally; or
  (b) in writing.

(2) The Minister must not give a Ministerial authorisation orally in relation to:
  (a) a cyber security incident; and
  (b) an asset;

  unless the delay that would occur if the Ministerial authorisation were to be made in writing would frustrate the effectiveness of:
  (c) any directions that may be given under section 35AK or 35AQ in relation to the incident and the asset; or

Authorised Version C2022C00160 registered 02/05/2022

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

Notification of Ministerial authorisations given orally

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

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

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

Authorised Version C2022C00160 registered 02/05/2022

Minister considers to be most relevant in relation to the Ministerial authorisation:

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

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

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

Notification of Ministerial authorisations given in writing

(6) If a Ministerial authorisation is given in writing in relation to:

(a) a cyber security incident; and

(b) an asset;

the Minister must:

(c) give a copy of the Ministerial authorisation to the Secretary and the Inspector-General of Intelligence and Security; and

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

(7) If a Ministerial authorisation is given in writing in relation to:

(a) a cyber security incident; and

(b) a critical infrastructure asset;

the Minister must:

(c) give a copy of the Ministerial authorisation to the responsible entity for the asset; and

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

(8) If a Ministerial authorisation is given in writing in relation to:

(a) a cyber security incident; and

(b) a critical infrastructure sector asset (other than a critical infrastructure asset);

the Minister must:

(c) give a copy of the Ministerial authorisation to whichever of the following entities the Minister considers to be most relevant in relation to the Ministerial authorisation:

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

Authorised Version C2022C00160 registered 02/05/2022

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

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

35AF Form of application for Ministerial authorisation

(1) The Secretary may apply for a Ministerial authorisation either:

(a) orally; or

(b) in writing.

(2) The Secretary must not apply orally for a Ministerial authorisation that relates to:

(a) a cyber security incident; and

(b) an asset;

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

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

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

(3) If an application for a Ministerial authorisation is made orally, the Secretary must:

(a) do both of the following:

(i) make a written record of the application;

(ii) give a copy of the written record of the application to the Minister; and

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

35AG Duration of Ministerial authorisation

Scope

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

(a) a cyber security incident; and

(b) an asset.

Authorised Version C2022C00160 registered 02/05/2022

Duration of Ministerial authorisation

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

Fresh Ministerial authorisation

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

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

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

35AH Revocation of Ministerial authorisation

Scope

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

Power to revoke Ministerial authorisation

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

Authorised Version C2022C00160 registered 02/05/2022

Duty to revoke Ministerial authorisation

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

(4) If the Secretary is satisfied that the Ministerial authorisation is no longer required to respond to the incident, the Secretary must:
  (a) notify the Minister that the Secretary is so satisfied; and
  (b) do so soon as practicable after the Secretary becomes so satisfied.

Notification of revocation

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

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

(7) If a Ministerial authorisation is revoked in relation to:
  (a) a cyber security incident; and
  (b) a critical infrastructure sector asset (other than a critical infrastructure asset);
the Minister must:

Authorised Version C2022C00160 registered 02/05/2022

(c) give a copy of the revocation to whichever of the following entities the Minister considers to be most relevant in relation to the Ministerial authorisation:
  (i) the owner, or each of the owners, of the asset;
  (ii) the operator, or each of the operators, of the asset; and
(d) do so within 48 hours after the Ministerial authorisation is revoked.

Revocation is not a legislative instrument

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

Application of Acts Interpretation Act 1901

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

35AJ Minister to exercise powers personally

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

Authorised Version C2022C00160 registered 02/05/2022

Division 3—Information gathering directions

35AK Information gathering direction

Scope

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

Direction

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

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

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

(4) The Secretary must not give the direction unless the Secretary is satisfied that:
  (a) the direction is a proportionate means of obtaining the information; and
  (b) compliance with the direction is technically feasible.

(5) The Secretary must not give a direction that would require an entity to:
  (a) do an act or thing that would be prohibited by section 7 of the *Telecommunications (Interception and Access) Act 1979*; or

Authorised Version C2022C00160 registered 02/05/2022

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

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

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

Other powers not limited

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

35AL Form of direction

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

(a) orally; or

(b) in writing.

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

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

(a) do both of the following:

(i) make a written record of the direction;

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

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

Authorised Version C2022C00160 registered 02/05/2022

35AM Compliance with an information gathering direction

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

Civil penalty: 150 penalty units.

35AN Self-incrimination etc.

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

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

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

35AP Admissibility of information etc.

If information is given under section 35AK:

(a) the information; or

(b) giving the information;

is not admissible in evidence against an entity:

(c) in criminal proceedings other than proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* that relates to this Act; or

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

Authorised Version C2022C00160 registered 02/05/2022

Division 4—Action directions

35AQ Action direction

(1) If an entity is a relevant entity for:
  (a) a critical infrastructure asset; or
  (b) a critical infrastructure sector asset;
the Secretary may give the entity a direction that directs the entity to do, or refrain from doing, a specified act or thing within the period specified in the direction.

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

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

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

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

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

Other powers not limited

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

Authorised Version C2022C00160 registered 02/05/2022

35AR Form of direction

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

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

(3) If a direction under section 35AQ is given orally to an entity, the Secretary must:
  (a) do both of the following:
    (i) make a written record of the direction;
    (ii) give a copy of the written record of the direction to the entity; and
  (b) do so within 48 hours after the direction is given.

35AS Revocation of direction

Scope

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

Power to revoke direction

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

Duty to revoke direction

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

Authorised Version C2022C00160 registered 02/05/2022

Automatic revocation of direction

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

Application of Acts Interpretation Act 1901

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

35AT Compliance with direction

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

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

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

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.

35AV Directions prevail over inconsistent obligations

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

Authorised Version C2022C00160 registered 02/05/2022

35AW Liability

(1) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with a direction given under section 35AQ.

(2) An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1).

(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

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

Division 5—Intervention requests

35AX Intervention request

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

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

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

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

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

(5) A request under this section does not extend to:
   (a) doing an act or thing that would be prohibited by section 7 of the *Telecommunications (Interception and Access) Act 1979*; or
   (b) doing an act or thing that would be prohibited by section 108 of the *Telecommunications (Interception and Access) Act 1979*; or
   (c) doing an act or thing that would (disregarding this Act) be prohibited by section 276, 277 or 278 of the *Telecommunications Act 1997*.

Authorised Version C2022C00160 registered 02/05/2022

Other powers not limited

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

35AY Form and notification of request

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

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

Notification of requests given orally

(3) If a request under section 35AX is given orally, the Secretary must:
  (a) do both of the following:
    (i) make a written record of the request;
    (ii) give a copy of the written record of the request to the chief executive of the authorised agency; and
  (b) do so within 48 hours after the request is given.

(4) If a request under section 35AX is given orally in relation to a critical infrastructure asset, the Secretary must:
  (a) do both of the following:
    (i) make a written record of the request;
    (ii) give a copy of the written record of the request to the responsible entity for the asset; and
  (b) do so within 48 hours after the request is given.

(5) If a request under section 35AX is given orally in relation to a critical infrastructure sector asset (other than a critical infrastructure asset), the Secretary must:
  (a) make a written record of the request; and

Authorised Version C2022C00160 registered 02/05/2022

(b) give a copy of the written record of the request to whichever of the following entities the Secretary considers to be most relevant in relation to the request:
  (i) the owner, or each of the owners, of the asset;
  (ii) the operator, or each of the operators, of the asset; and
(c) do so within 48 hours after the request is given.

Notification of requests given in writing

(6) If a request under section 35AX is given in writing, the Secretary must:
  (a) give a copy of the request to the chief executive of the authorised agency; and
  (b) do so within 48 hours after the request is made.

(7) If a request under section 35AX is given in writing in relation to a critical infrastructure asset, the Secretary must:
  (a) give a copy of the request to the responsible entity for the asset; and
  (b) do so within 48 hours after the request is given.

(8) If a request under section 35AX is given in writing in relation to a critical infrastructure sector asset (other than a critical infrastructure asset), the Secretary must:
  (a) give a copy of the request to whichever of the following entities the Secretary considers to be most relevant in relation to the request:
    (i) the owner, or each of the owners, of the asset;
    (ii) the operator, or each of the operators, of the asset; and
  (b) do so within 48 hours after the request is given.

35AZ Compliance with request

(1) The authorised agency is authorised to do an act or thing in compliance with a request under section 35AX.

(2) An act or thing done by the authorised agency in compliance with a request under section 35AX is taken to be done in the performance

Authorised Version C2022C00160 registered 02/05/2022

of the function conferred on the authorised agency by paragraph 7(1)(f) of the *Intelligence Services Act 2001*.

35BA Revocation of request

Scope

(1) This section applies if a request is in force under section 35AX in relation to a Ministerial authorisation.

Power to revoke request

(2) The Secretary may, by written notice given to the chief executive of the authorised agency, revoke the request.

Duty to revoke request

(3) If the Secretary is satisfied that the request is no longer required to respond to the cyber security incident to which the Ministerial authorisation relates, the Secretary must, by written notice given to the chief executive of the authorised agency, revoke the request.

Automatic revocation of request

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

Notification of revocation of request

(5) If a request under section 35AX is revoked, the Secretary must:
   (a) give a copy of the revocation of the request to the chief executive of the authorised agency and each relevant entity for the asset; and
   (b) do so as soon as practicable after the revocation.

Application of Acts Interpretation Act 1901

(6) This section does not, by implication, affect the application of subsection 33(3) of the *Acts Interpretation Act 1901* to an

Authorised Version C2022C00160 registered 02/05/2022

instrument made under a provision of this Act (other than this Part).

35BB Relevant entity to assist the authorised agency

(1) If:

(a) a request is in force under section 35AX in relation to a critical infrastructure asset or a critical infrastructure sector asset; and

(b) an entity is a relevant entity for the asset;

an approved staff member of the authorised agency may require the entity to:

(c) provide the approved staff member with access to premises for the purposes of the authorised agency complying with the request; or

(d) provide the authorised agency with specified information or assistance that is reasonably necessary to allow the authorised agency to comply with the request.

Note: See also section 149.1 of the *Criminal Code* (which deals with obstructing and hindering Commonwealth public officials).

(2) Paragraph (1)(c) does not apply to premises that are used solely or primarily as a residence.

(3) An entity must comply with a requirement under subsection (1).

Civil penalty: 150 penalty units.

Liability

(4) An entity is not liable to an action or other proceeding for damages for, or in relation to, an act done or omitted in good faith in compliance with a requirement under subsection (1).

(5) An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for, or in relation to, an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (4).

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

35BC Constable may assist the authorised agency

(1) If an entity refuses or fails to provide an approved staff member of the authorised agency with access to premises when required to do so under subsection 35BB(1):
  (a) the approved staff member may enter the premises for the purposes of the authorised agency complying with the request mentioned in that subsection; and
  (b) a constable may:
    (i) assist the approved staff member in gaining access to the premises by using reasonable force against property; and
    (ii) if necessary for the purposes of so assisting the approved staff member—enter the premises.

(2) If an approved staff member of the authorised agency has entered premises for the purposes of the authorised agency complying with a request under section 35AX, a constable may:
  (a) assist the authorised agency in complying with the request by using reasonable force against property located on the premises; and
  (b) for the purposes of so assisting the authorised agency—enter the premises.

35BD Removal and return of computers etc.

Removal of computers etc.

(1) If:
  (a) in compliance with a request under section 35AX, the authorised agency adds or connects a computer or device to a computer network; and
  (b) at a time when the request is in force, an approved staff member of the authorised agency forms a reasonable belief that the addition or connection of the computer or device is no longer required for the purposes of responding to the

Authorised Version C2022C00160 registered 02/05/2022

cyber security incident to which the relevant Ministerial authorisation relates;

the authorised agency must remove or disconnect the computer or device as soon as practicable after the approved staff member forms that belief.

(2) If:

(a) in compliance with a request under section 35AX, the authorised agency adds or connects a computer or device to a computer network; and

(b) the request ceases to be in force;

the authorised agency must remove or disconnect the computer or device as soon as practicable after the request ceases to be in force.

Return of computers etc.

(3) If:

(a) in compliance with a request under section 35AX, the authorised agency removes a computer or device; and

(b) at a time when the request is in force, an approved staff member of the authorised agency forms a reasonable belief that the removal of the computer or device is no longer required for the purposes of responding to the cyber security incident to which the relevant Ministerial authorisation relates;

the authorised agency must return the computer or device as soon as practicable after the approved staff member forms that belief.

(4) If:

(a) in compliance with a request under section 35AX, the authorised agency removes a computer or device; and

(b) the request ceases to be in force;

the authorised agency must return the computer or device as soon as practicable after the request ceases to be in force.

Authorised Version C2022C00160 registered 02/05/2022

35BE Use of force against an individual not authorised

This Division does not authorise the use of force against an individual.

35BF Liability

Each of the following:

(a) the chief executive of the authorised agency;

(b) an approved staff member of the authorised agency;

(c) a constable;

is not liable to an action or other proceeding (whether civil or criminal) for, or in relation to, an act or matter done or omitted to be done in the exercise of any power or authority conferred by this Division.

35BG Evidentiary certificates

(1) The Inspector-General of Intelligence and Security may issue a written certificate setting out any facts relevant to the question of whether anything done, or omitted to be done, by the authorised agency, or an approved staff member of the authorised agency, was done, or omitted to be done, in the exercise of any power or authority conferred by this Division.

(2) A certificate issued under subsection (1) is admissible in evidence in any proceedings as prima facie evidence of the matters stated in the certificate.

35BH Chief executive of the authorised agency to report to the Defence Minister and the Minister

(1) If:

(a) the Secretary gives a request under section 35AX that was authorised by a Ministerial authorisation; and

(b) the authorised agency does one or more acts or things in compliance with the request;

the chief executive of the authorised agency must:

Authorised Version C2022C00160 registered 02/05/2022

(c) prepare a written report that:
  (i) sets out details of those acts or things; and
  (ii) explains the extent to which doing those acts or things has amounted to an effective response to the cyber security incident to which the Ministerial authorisation relates; and
(d) give a copy of the report to the Defence Minister; and
(e) give a copy of the report to the Minister.

(2) The chief executive of the authorised agency must comply with subsection (1) as soon as practicable after the end of the period specified in the request and, in any event, within 3 months after the end of the period specified in the request.

35BJ Approved staff members of the authorised agency

(1) The chief executive of the authorised agency may, in writing, declare that a specified staff member of the authorised agency is an ***approved staff member of the authorised agency*** for the purposes of this Act.

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

Authorised Version C2022C00160 registered 02/05/2022

Division 6—Reports to the Parliamentary Joint Committee on Intelligence and Security

35BK Reports to the Parliamentary Joint Committee on Intelligence and Security

(1) If the Secretary gives one or more directions under section 35AK or 35AQ, or one or more requests under section 35AX, in relation to a cyber security incident, the Secretary must give the Parliamentary Joint Committee on Intelligence and Security a written report about the incident.

(2) The report must include a description of each of the directions or requests.

Authorised Version C2022C00160 registered 02/05/2022

Part 4—Gathering and using information

Division 1—Simplified outline of this Part

36 Simplified outline of this Part

The Secretary may require a reporting entity for, or an operator of, a critical infrastructure asset to provide certain information or documents.

The making of a record, or the use or disclosure, of protected information is authorised in particular circumstances but is otherwise an offence.

The privilege against self-incrimination does not apply in relation to a requirement to provide information or documents under this Part.

Note: Protected information is defined in section 5.

Authorised Version C2022C00160 registered 02/05/2022

Division 2—Secretary's power to obtain information or documents

37 Secretary may obtain information or documents from entities

(1) This section applies if the Secretary has reason to believe that an entity that is a reporting entity for, or an operator of, a critical infrastructure asset has information or a document that:
   (a) is relevant to the exercise of a power, or the performance of a duty or function, under this Act in relation to the asset; or
   (b) may assist with determining whether a power under this Act should be exercised in relation to the asset.

Requirement to give information or documents

(2) The Secretary may, by notice in writing given to the entity, require the entity to:
   (a) give any such information; or
   (b) produce any such documents; or
   (c) make copies of any such documents and to produce those copies;

   to the Secretary within the period, and in the manner, specified in the notice.

Matters to which regard must be had

(3) Before giving the entity the notice, the Secretary:
   (a) must have regard to the costs that would be likely to be incurred by the entity in complying with the notice; and
   (b) may have regard to any other matters the Secretary considers relevant.

Compliance with notice

(4) An entity must comply with a notice given to the entity under subsection (2).

Authorised Version C2022C00160 registered 02/05/2022

Note 1: This subsection is not subject to the privilege against self-incrimination, but there are limits on the uses to which the information, document or copy may be put (see section 40).

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

Civil penalty: 150 penalty units.

Matters to be set out in notice

(5) The notice must set out the effect of the following provisions:
  (a) subsection (4);
  (b) Part 5 (enforcement);
  (c) sections 137.1 and 137.2 of the *Criminal Code* (false or misleading information or documents).

Compensation for producing copies of documents

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

38 Copies of documents

(1) The Secretary may inspect a document or copy produced under section 37 and may make and retain copies of such a document.

(2) The Secretary may retain possession of a copy of a document produced in accordance with a requirement covered by paragraph 37(2)(c).

39 Retention of documents

(1) The Secretary may take, and retain for as long as is necessary, possession of a document produced under section 37.

(2) The entity otherwise entitled to possession of the document is entitled to be supplied, as soon as practicable, with a copy certified by the Secretary to be a true copy.

Authorised Version C2022C00160 registered 02/05/2022

(3) The certified copy must be received in all courts and tribunals as evidence as if it were the original.

(4) Until a certified copy is supplied, the Secretary must, at such times and places as the Secretary thinks appropriate, permit the entity otherwise entitled to possession of the document, or a person authorised by that entity, to inspect and make copies of the document.

40 Self-incrimination

(1) An entity is not excused from giving information or producing a document or copy of a document under subsection 37(4) on the ground that the information or the production of the document or copy might tend to incriminate the entity or expose the entity to a penalty.

(2) However, in the case of an individual:
  (a) the information given or the document or copy produced; or
  (b) giving the information or producing the document or copy; or
  (c) any information, document or thing obtained as a direct or indirect consequence of giving the information or producing the document or copy;

  is not admissible in evidence against the individual:
  (d) in criminal proceedings other than proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* that relates to this Act; or
  (e) in civil proceedings other than proceedings for recovery of a penalty in relation to a contravention of subsection 37(4).

Authorised Version C2022C00160 registered 02/05/2022

Division 3—Use and disclosure of protected information

Subdivision A—Authorised use and disclosure

41 Authorised use and disclosure—performing functions etc.

An entity may make a record of, use or disclose protected information if the entity makes the record, or uses or discloses the information, for the purposes of:

(a) exercising the entity's powers, or performing the entity's functions or duties, under this Act; or

(b) otherwise ensuring compliance with a provision of this Act.

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

42 Authorised use and disclosure—other person's functions etc.

(1) The Secretary may:

(a) disclose protected information to a person mentioned in subsection (2); and

(b) make a record of or use protected information for the purpose of that disclosure;

for the purposes of enabling or assisting the person to exercise his or her powers or perform his or her functions or duties.

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

(2) The persons to whom the Secretary may disclose protected information are the following:

(a) a Minister of the Commonwealth who has responsibility for any of the following:

(i) national security;

(ii) law enforcement;

(iii) foreign investment in Australia;

(iv) taxation policy;

Authorised Version C2022C00160 registered 02/05/2022

(v) industry policy;
(vi) promoting investment in Australia;
(vii) defence;
(viii) the regulation or oversight of the relevant critical infrastructure sector to which the protected information relates;

(b) 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;

(c) a person employed as a member of staff of a Minister mentioned in paragraph (a) or (b);

(d) the head of an agency (including a Department) administered by a Minister mentioned in paragraph (a) or (b), or an officer or employee of that agency.

42A Authorised use and disclosure—development of proposed amendments of this Act etc.

The Secretary may:

(a) disclose protected information to an entity for the purposes of developing or assessing:
(i) proposed amendments of this Act; or
(ii) proposed rules; or
(iii) proposed amendments of the rules; and

(b) make a record of or use protected information for the purpose of that disclosure.

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

43 Authorised disclosure relating to law enforcement

The Secretary may disclose protected information to an enforcement body (within the meaning of the *Privacy Act 1988*) for the purposes of one or more enforcement related activities (within

Authorised Version C2022C00160 registered 02/05/2022

the meaning of that Act) conducted by or on behalf of the enforcement body.

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

43AA Authorised disclosure to Ombudsman official

The Secretary may:

(a) disclose protected information to an Ombudsman official for the purposes of exercising powers, or performing duties or functions, as an Ombudsman official; and

(b) make a record of or use protected information for the purpose of that disclosure.

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

43A Authorised disclosure to IGIS official

The Secretary may:

(a) disclose protected information to an IGIS official for the purposes of exercising powers, or performing duties or functions, as an IGIS official; and

(b) make a record of or use protected information for the purpose of that disclosure.

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

43B Authorised use and disclosure—Ombudsman official

Protected information may be disclosed by an Ombudsman official to an IGIS official for the purposes of the IGIS official exercising powers, or performing functions or duties, as an IGIS official.

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

Authorised Version C2022C00160 registered 02/05/2022

43C Authorised use and disclosure—IGIS official

Protected information may be disclosed by an IGIS official to an Ombudsman official for the purposes of the Ombudsman official exercising powers, or performing functions or duties, as an Ombudsman official.

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

43D Authorised use and disclosure—ASD

The Director-General of ASD or a staff member of ASD may make a record of, use or disclose protected information for the purposes of the performance of the functions of ASD set out in section 7 of the *Intelligence Services Act 2001*.

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

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);

Authorised Version C2022C00160 registered 02/05/2022

(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.

Authorised Version C2022C00160 registered 02/05/2022

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

44 Secondary use and disclosure of protected information

An entity may make a record of, use or disclose protected information if:

(a) the entity obtains the information under this Subdivision (including this section); and

(b) the entity makes the record, or uses or discloses the information, for the purposes for which the information was disclosed to the entity.

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

Subdivision B—Offence for unauthorised use or disclosure

45 Offence for unauthorised use or disclosure of protected information

(1) An entity commits an offence if:

(a) the entity:

(i) obtains information; or

(ii) generates information for the purposes of complying with this Act; and

(b) the information is protected information; and

(c) the entity makes a record of, discloses or otherwise uses the information; and

(d) the making of the record, or the disclosure or use, is not authorised under Subdivision A or required by a notification provision.

Note 1: For exceptions to this offence, see section 46.

Note 2: Information includes the fact that an asset is declared under section 51 to be a critical infrastructure asset (see the definition of ***protected information*** in section 5).

Note 3: If the entity is not a legal person, see Division 2 of Part 7.

Authorised Version C2022C00160 registered 02/05/2022

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

(2) Section 15.1 of the *Criminal Code* (extended geographical jurisdiction—category A) applies to an offence against subsection (1).

46 Exceptions to offence for unauthorised use or disclosure

Required or authorised by law

(1) Section 45 does not apply if the making of the record, or the disclosure or use, of the information is required or authorised by or under:
   (a) a law of the Commonwealth, other than Subdivision A or a notification provision; or
   (b) a law of a State or Territory prescribed by the rules.

(2) For the purposes of subsection (1) of this section, the following laws:
   (a) the *Corporations Act 2001*, except a provision of that Act prescribed by the rules;
   (b) a law, or a provision of a law, of the Commonwealth prescribed by the rules;

   are taken not to require or authorise the making of a record, or the disclosure, of the fact that an asset is declared under section 51 to be a critical infrastructure asset or of the fact that an asset is declared under section 52B to be a system of national significance.

Good faith

(3) Section 45 does not apply to an entity to the extent that the entity makes a record of, discloses or otherwise uses protected information in good faith and in purported compliance with Subdivision A or a notification provision.

Person to whom the protected information relates

(4) Section 45 does not apply to an entity if:

Authorised Version C2022C00160 registered 02/05/2022

(a) the entity discloses protected information to the entity to whom the information relates; or

(c) the making of the record, or the disclosure or use, of the protected information is in accordance with the express or implied consent of the entity to whom the information relates.

Disclosure to an Ombudsman official

(5) Section 45 does not apply to an entity to the extent that the entity discloses protected information to an Ombudsman official for the purposes of exercising powers, or performing duties or functions, as an Ombudsman official.

Note: A defendant bears an evidential burden in relation to the matters in this section (see subsection 13.3(3) of the *Criminal Code*).

47 No requirement to provide information

(1) An entity is not (subject to subsection (2)) to be required to disclose protected information, or produce a document containing protected information, to:

(a) a court; or

(b) a tribunal, authority or person that has the power to require the answering of questions or the production of documents.

(2) Subsection (1) does not prevent an entity from being required to disclose protected information, or to produce a document containing protected information, if it is necessary to do so for the purposes of giving effect to:

(a) this Act; or

(b) the *Inspector-General of Intelligence and Security Act 1986*, or any other Act that confers functions, powers or duties on the Inspector-General of Intelligence and Security; or

(c) a legislative instrument made under an Act mentioned in paragraph (a) or (b).

Authorised Version C2022C00160 registered 02/05/2022

Part 5—Enforcement

Division 1—Simplified outline of this Part

48 Simplified outline of this Part

Civil penalty orders may be sought under Part 4 of the Regulatory Powers Act in relation to contraventions of civil penalty provisions of this Act.

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

Injunctions under Part 7 of that Act may be used to restrain a person from contravening a civil penalty provision of this Act or to compel compliance with a civil penalty provision of this Act.

Infringement notices may be given under Part 5 of the Regulatory Powers Act for alleged contraventions of certain provisions of this Act.

A provision is subject to monitoring under Part 2 of the Regulatory Powers Act if it is:

(a) an offence against section 35AT or 45 of this Act; or
(b) a civil penalty provision of this Act.

A provision is subject to investigation under Part 3 of the Regulatory Powers Act if it is:

(a) an offence against section 35AT or 45 of this Act; or
(b) a civil penalty provision of this Act.

Authorised Version C2022C00160 registered 02/05/2022

Division 2—Civil penalties, enforceable undertakings and injunctions

49 Civil penalties, enforceable undertakings and injunctions

Enforceable provisions

(1) Each civil penalty provision of this Act is enforceable under:
  (a) Part 4 of the Regulatory Powers Act (civil penalty provisions); and
  (b) Part 6 of that Act (enforceable undertakings); and
  (c) Part 7 of that Act (injunctions).

Note 1: Part 4 of the Regulatory Powers Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

Note 2: Part 6 of that Act creates a framework for accepting and enforcing undertakings relating to compliance with provisions.

Note 3: Part 7 of that Act creates a framework for using injunctions to enforce provisions.

Authorised applicant

(2) For the purposes of Part 4 of the Regulatory Powers Act, as that Part applies in relation to a civil penalty provision of this Act, each of the following persons is an authorised applicant:
  (a) the Secretary;
  (b) a person who is appointed under subsection (3).

(3) The Secretary may, by writing, appoint a person who:
  (a) is the chief executive officer (however described) of a relevant Commonwealth regulator; or
  (b) is an SES employee, or an acting SES employee, in:
    (i) the Department; or
    (ii) a relevant Commonwealth regulator; or

Authorised Version C2022C00160 registered 02/05/2022

(c) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant for the purposes of Part 4 of the Regulatory Powers Act, as that Part applies in relation to a civil penalty provision of this Act.

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

Authorised person

(3A) For the purposes of Parts 6 and 7 of the Regulatory Powers Act, as those Parts apply in relation to a civil penalty provision of this Act, each of the following persons is an authorised applicant:

(a) the Secretary;

(b) a person who is appointed under subsection (3B).

(3B) The Secretary may, by writing, appoint a person who:

(a) is the chief executive officer (however described) of a relevant Commonwealth regulator; or

(b) is an SES employee, or an acting SES employee, in:

(i) the Department; or

(ii) a relevant Commonwealth regulator; or

(c) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant for the purposes of Parts 6 and 7 of the Regulatory Powers Act, as those Parts apply in relation to a civil penalty provision of this Act.

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

Relevant court

(4) For the purposes of Parts 4, 6 and 7 of the Regulatory Powers Act, as those Parts apply in relation to a civil penalty provision of this Act, each of the following is a relevant court:

Authorised Version C2022C00160 registered 02/05/2022

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

Extension outside Australia

(5) Parts 4, 6 and 7 of the Regulatory Powers Act, as those Parts apply in relation to a civil penalty provision of this Act, extends outside Australia (including to every external Territory).

Authorised Version C2022C00160 registered 02/05/2022

Division 3—Monitoring and investigation powers

49A Monitoring powers

Provisions subject to monitoring

(1) A provision is subject to monitoring under Part 2 of the Regulatory Powers Act if it is:
  (a) an offence against section 35AT or 45; or
  (b) a civil penalty provision of this Act.

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

Information subject to monitoring

(2) Information given in compliance or purported compliance with a provision of this Act is subject to monitoring under Part 2 of the Regulatory Powers Act.

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

Authorised applicant

(3) For the purposes of Part 2 of the Regulatory Powers Act, a person who is appointed under subsection (4) is an authorised applicant in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

(4) The Secretary may, by writing, appoint a person who:
  (a) is an SES employee, or an acting SES employee, in:
    (i) the Department; or
    (ii) a relevant Commonwealth regulator; or
  (b) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

Authorised Version C2022C00160 registered 02/05/2022

to be an authorised applicant in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

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

Authorised person

(5) For the purposes of Part 2 of the Regulatory Powers Act, a person who is appointed under subsection (6) is an authorised person in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

(6) The Secretary may, by writing, appoint a person who is:
  (a) an APS employee in:
    (i) the Department; or
    (ii) a relevant Commonwealth regulator; or
  (b) an officer or employee of a relevant Commonwealth regulator;

to be an authorised person in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

Issuing officer

(7) For the purposes of Part 2 of the Regulatory Powers Act, a magistrate is an issuing officer in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

Relevant chief executive

(8) For the purposes of Part 2 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

(9) The relevant chief executive may, in writing, delegate the powers and functions mentioned in subsection (10) to a person who is an SES employee, or an acting SES employee, in the Department.

Authorised Version C2022C00160 registered 02/05/2022

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

(10) The powers and functions that may be delegated are:
  (a) powers under Part 2 of the Regulatory Powers Act in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2); and
  (b) powers and functions under the Regulatory Powers Act that are incidental to a power mentioned in paragraph (a).

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

Relevant court

(12) For the purposes of Part 2 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2):
  (a) the Federal Court of Australia;
  (b) the Federal Circuit and Family Court of Australia (Division 2); and
  (c) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

Premises

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

Person assisting

(14) An authorised person may be assisted by other persons in exercising powers, or performing functions or duties, under Part 2 of the Regulatory Powers Act in relation to the provisions

Authorised Version C2022C00160 registered 02/05/2022

mentioned in subsection (1) and information mentioned in subsection (2).

External Territories

(15) Part 2 of the Regulatory Powers Act, as it applies in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2), extends to every external Territory.

49B Investigation powers

Provisions subject to investigation

(1) A provision is subject to investigation under Part 3 of the Regulatory Powers Act if it is:
  (a) an offence against section 35AT or 45; or
  (b) a civil penalty provision of this Act.

Authorised applicant

(2) For the purposes of Part 3 of the Regulatory Powers Act, a person who is appointed under subsection (3) is an authorised applicant in relation to evidential material that relates to a provision mentioned in subsection (1).

(3) The Secretary may, by writing, appoint a person who:
  (a) is an SES employee, or an acting SES employee, in:
    (i) the Department; or
    (ii) a relevant Commonwealth regulator; or
  (b) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant in relation to evidential material that relates to a provision mentioned in subsection (1).

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

Authorised Version C2022C00160 registered 02/05/2022

Authorised person

(4) For the purposes of Part 3 of the Regulatory Powers Act, a person who is appointed under subsection (5) is an authorised person in relation to evidential material that relates to a provision mentioned in subsection (1).

(5) The Secretary may, by writing, appoint a person who is:
  (a) an APS employee in:
    (i) the Department; or
    (ii) a relevant Commonwealth regulator; or
  (b) an officer or employee of a relevant Commonwealth regulator;

to be an authorised person in relation to evidential material that relates to a provision mentioned in subsection (1).

Issuing officer

(6) For the purposes of Part 3 of the Regulatory Powers Act, a magistrate is an issuing officer in relation to evidential material that relates to a provision mentioned in subsection (1).

Relevant chief executive

(7) For the purposes of Part 3 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to evidential material that relates to a provision mentioned in subsection (1).

(8) The relevant chief executive may, in writing, delegate the powers and functions mentioned in subsection (9) to a person who is an SES employee or an acting SES employee in the Department.

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

(9) The powers and functions that may be delegated are:
  (a) powers under Part 3 of the Regulatory Powers Act in relation to evidential material that relates to a provision mentioned in subsection (1); and

Authorised Version C2022C00160 registered 02/05/2022

(b) powers and functions under the Regulatory Powers Act that are incidental to a power mentioned in paragraph (a).

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

Relevant court

(11) For the purposes of Part 3 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to evidential material that relates to a provision mentioned in subsection (1):

(a) the Federal Court of Australia;

(b) the Federal Circuit and Family Court of Australia (Division 2);

(c) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

Person assisting

(12) An authorised person may be assisted by other persons in exercising powers, or performing functions or duties, under Part 3 of the Regulatory Powers Act in relation to evidential material that relates to a provision mentioned in subsection (1).

External Territories

(13) Part 3 of the Regulatory Powers Act, as it applies in relation to the provisions mentioned in subsection (1), extends to every external Territory.

Authorised Version C2022C00160 registered 02/05/2022

Division 4—Infringement notices

49C Infringement notices

Provisions subject to an infringement notice

(1) A civil penalty provision of this Act is subject to an infringement notice under Part 5 of the Regulatory Powers Act.

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

Infringement officer

(2) For the purposes of Part 5 of the Regulatory Powers Act, a person authorised under subsection (3) is an infringement officer in relation to the provisions mentioned in subsection (1).

(3) The Secretary may, by writing, authorise a person who:
  (a) is an SES employee, or an acting SES employee, in:
    (i) the Department; or
    (ii) a relevant Commonwealth regulator; or
  (b) holds, or is acting in, a position in a relevant Commonwealth regulator that is equivalent to, or higher than, a position occupied by an SES employee;

to be an infringement officer in relation to the provisions mentioned in subsection (1).

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

Relevant chief executive

(4) For the purposes of Part 5 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to the provisions mentioned in subsection (1).

(5) The relevant chief executive may, in writing, delegate any or all of the relevant chief executive's powers and functions under Part 5 of

Authorised Version C2022C00160 registered 02/05/2022

the Regulatory Powers Act to a person who is an SES employee or an acting SES employee in the Department.

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

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

External Territories

(7) Part 5 of the Regulatory Powers Act, as it applies in relation to the provisions mentioned in subsection (1), extends to every external Territory.

Authorised Version C2022C00160 registered 02/05/2022

Part 6—Declaration of assets by the Minister

Division 1—Simplified outline of this Part

50 Simplified outline of this Part

The Minister may privately declare an asset to be a critical infrastructure asset if the Minister is satisfied that:

(a) the asset is critical infrastructure that affects national security; and

(b) there would be a risk to national security if it were publicly known that the asset is critical infrastructure that affects national security.

The Minister must notify each reporting entity for a declared asset.

If a reporting entity for a declared asset ceases to be such a reporting entity, or becomes aware of another reporting entity for the asset, the entity must notify the Secretary.

It is an offence to disclose that an asset has been so declared (see section 45).

Authorised Version C2022C00160 registered 02/05/2022

Division 2—Declaration of assets by the Minister

51 Declaration of assets by the Minister

(1) The Minister may, in writing, declare a particular asset to be a critical infrastructure asset if:
  (a) the asset is not otherwise a critical infrastructure asset; and
  (b) the asset relates to a critical infrastructure sector; and
  (c) the Minister is satisfied that the asset is critical to:
    (i) the social or economic stability of Australia or its people; or
    (ii) the defence of Australia; or
    (iii) national security; and
  (d) there would be a risk to:
    (i) the social or economic stability of Australia or its people; or
    (ii) the defence of Australia; or
    (iii) national security;

  if it were publicly known that the asset is a critical infrastructure asset.

Note: It is an offence to disclose the fact that an asset is declared to be a critical infrastructure asset (see section 45).

(2) The declaration must specify the entity that is the responsible entity for the asset.

(2A) The declaration may do any or all of the following:
  (a) determine that Part 2 applies to the asset;
  (b) determine that Part 2A applies to the asset;
  (c) determine that Part 2B applies to the asset.

(3) The Minister must notify the following of the declaration, in writing, within 30 days after making the declaration:
  (a) each reporting entity for the asset;

Authorised Version C2022C00160 registered 02/05/2022

(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.

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

51A Consultation—declaration

(1) Before making a declaration under section 51 that specifies an entity as the responsible entity for an asset, the Minister must give the entity a notice:
  (a) setting out the proposed declaration; and
  (b) inviting the entity to make submissions to the Minister about the proposed declaration within:
    (i) 28 days after the notice is given; or
    (ii) if a shorter period is specified in the notice—that shorter period.

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

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

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

52 Notification of change to reporting entities for asset

(1) This section applies if a reporting entity (the ***first entity***) for an asset declared under subsection 51(1) to be a critical infrastructure asset:

Authorised Version C2022C00160 registered 02/05/2022

(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).

(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).

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

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 51(1), in writing, within 30 days after being notified under that paragraph.

Authorised Version C2022C00160 registered 02/05/2022

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).

Authorised Version C2022C00160 registered 02/05/2022

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;
  (aa) the Parliamentary Joint Committee on Intelligence and Security;
  (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

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

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.

Authorised Version C2022C00160 registered 02/05/2022

Part 7—Miscellaneous

Division 1—Simplified outline of this Part

53 Simplified outline of this Part

This Act applies to partnerships, trusts, superannuation funds and unincorporated foreign companies (amongst other entities), but with some modifications.

The Secretary has certain powers and obligations under this Part, including the power to undertake an assessment of a critical infrastructure asset to determine if there is a risk to national security relating to the asset.

The Secretary must give the Minister a report each financial year for presentation to the Parliament. The report relates to the operation of this Act.

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

Authorised Version C2022C00160 registered 02/05/2022

Division 2—Treatment of certain entities

53A How certain entities hold interests

For the purposes of this Act, a trust, partnership, superannuation fund or unincorporated foreign company (as the case requires) is taken to hold an interest in an asset or entity if:

(a) one or more trustees hold the interest on behalf of the beneficiaries of the trust; or

(b) one or more partners hold the interest on behalf of the partnership; or

(c) one or more trustees hold the interest on behalf of the beneficiaries of the superannuation fund; or

(d) one or more appointed officers hold the interest on behalf of the company.

Note: For the definition of ***appointed officer***, see section 5.

54 Treatment of partnerships

(1) This Act applies to a partnership as if it were an entity, but with the changes set out in this section.

(2) An obligation that would otherwise be imposed on the partnership by this Act is imposed on each partner instead, but may be discharged by any of the partners.

(3) An offence against this Act that would otherwise have been committed by the partnership is taken to have been committed by each partner in the partnership, at the time the offence was committed, who:

(a) did the relevant act or made the relevant omission; or

(b) aided, abetted, counselled or procured the relevant act or omission; or

(c) was in any way knowingly concerned in, or party to, the relevant act or omission (whether directly or indirectly and whether by any act or omission of the partner).

Authorised Version C2022C00160 registered 02/05/2022

(4) This section applies to a contravention of a civil penalty provision in a corresponding way to the way in which it applies to an offence.

(5) For the purposes of this Act, a change in the composition of a partnership does not affect the continuity of the partnership.

55 Treatment of trusts and superannuation funds that are trusts

(1) This Act applies to a trust or a superannuation fund that is a trust as if it were an entity, but with the changes set out in this section.

Trusts or superannuation funds with a single trustee

(2) If the trust or superannuation fund has a single trustee:
  (a) an obligation that would otherwise be imposed on the trust or superannuation fund by this Act is imposed on the trustee instead; and
  (b) an offence against this Act that would otherwise have been committed by the trust or superannuation fund is taken to have been committed by the trustee.

Trusts or superannuation funds with multiple trustees

(3) If the trust or superannuation fund has 2 or more trustees:
  (a) an obligation that would otherwise be imposed on the trust or superannuation fund by this Act is imposed on each trustee instead, but may be discharged by any of the trustees; and
  (b) an offence against this Act that would otherwise have been committed by the trust or superannuation fund is taken to have been committed by each trustee of the trust or superannuation fund, at the time the offence was committed, who:
    (i) did the relevant act or made the relevant omission; or
    (ii) aided, abetted, counselled or procured the relevant act or omission; or

Authorised Version C2022C00160 registered 02/05/2022

(iii) was in any way knowingly concerned in, or party to, the relevant act or omission (whether directly or indirectly and whether by any act or omission of the trustee).

Contraventions of civil penalty provisions

(4) This section applies to a contravention of a civil penalty provision in a corresponding way to the way in which it applies to an offence.

56 Treatment of unincorporated foreign companies

(1) This Act applies to an unincorporated foreign company as if it were an entity, but with the changes set out in this section.

(2) An obligation that would otherwise be imposed on the unincorporated foreign company by this Act is imposed on each appointed officer for the company instead, but may be discharged by any of the appointed officers.

Note: For the definition of ***appointed officer***, see section 5.

(3) An offence against this Act that would otherwise have been committed by the unincorporated foreign company is taken to have been committed by each appointed officer for the company, at the time the offence was committed, who:

(a) did the relevant act or made the relevant omission; or

(b) aided, abetted, counselled or procured the relevant act or omission; or

(c) was in any way knowingly concerned in, or party to, the relevant act or omission (whether directly or indirectly and whether by any act or omission of the appointed officer).

(4) This section applies to a contravention of a civil penalty provision in a corresponding way to the way in which it applies to an offence.

Authorised Version C2022C00160 registered 02/05/2022

Division 3—Matters relating to Secretary's powers

57 Additional power of Secretary

Without limiting any other provision of this Act, the Secretary may undertake an assessment of a critical infrastructure asset to determine if there is a risk to national security relating to the asset.

58 Assets ceasing to be critical infrastructure assets

The Secretary must, in writing, notify the reporting entity for an asset if the Secretary becomes aware that the asset has ceased to be a critical infrastructure asset.

59 Delegation of Secretary's powers

(1) The Secretary may, by written instrument, delegate to an SES employee, or an acting SES employee, in the Department any of the Secretary's powers, functions or duties under this Act (other than Part 3A).

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

(2) In exercising powers, performing functions or discharging duties under a delegation, the delegate must comply with any written direction given by the Secretary to the delegate.

Authorised Version C2022C00160 registered 02/05/2022

Division 4—Periodic reports, reviews and rules etc.

60 Periodic report

(1) The Secretary must give the Minister, for presentation to the Parliament, a report on the operation of this Act for a financial year.

(2) Without limiting subsection (1), the report must deal with:

(a) the number of notifications that were made during the financial year to the Secretary under Division 3 of Part 2 (obligation to give information and notify of events); and

(b) any directions given during the financial year by the Minister under section 32 (direction if risk of act or omission that would be prejudicial to security); and

(c) the use during the financial year of the Secretary's powers under Division 2 of Part 4 (Secretary's power to obtain information or documents); and

(d) any action taken during the financial year against an entity under the Regulatory Powers Act as a result of Part 5 (enforcement) of this Act; and

(e) the number of declarations of assets as critical infrastructure assets that were made during the financial year by the Minister under section 51; and

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

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

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

(h) the number of cyber security incidents reported during the financial year under section 30BC; and

(i) the number of cyber security incidents reported during the financial year under 30BD; and

Authorised Version C2022C00160 registered 02/05/2022

(j) the number of notices given to entities under section 30CB during the financial year; and
(k) the number of notices given to entities under section 30CM during the financial year; and
(l) the number of notices given to entities under section 30CU during the financial year; and
(m) the number of notices given to entities under Division 5 of Part 2C during the financial year; and
(n) the number of Ministerial authorisations given under section 35AB during the financial year; and
(o) the number of Ministerial authorisations given under paragraph 35AB(2)(a) or (b) during the financial year; and
(p) the number of Ministerial authorisations given under paragraph 35AB(2)(c) or (d) during the financial year; and
(q) the number of Ministerial authorisations given under paragraph 35AB(2)(e) or (f) during the financial year; and
(r) the number of declarations of assets as systems of national significance that were made under section 52B during the financial year.

(3) A report under subsection (1) must not include personal information (within the meaning of the *Privacy Act 1988*).

Note: See also section 34C of the *Acts Interpretation Act 1901*, which contains extra rules about periodic reports.

60AAA Regular reports about consultation

(1) The Secretary must give the Minister a report relating to the conduct, progress and outcomes of consultations undertaken by the Department in relation to:
(a) the amendments made by the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*; and
(b) the amendments of this Act made by the *Security Legislation Amendment (Critical Infrastructure) Act 2021*;
during a designated reporting period (see subsection (4)).

Authorised Version C2022C00160 registered 02/05/2022

(2) The Minister must give a copy of a report under subsection (1) to the Parliamentary Joint Committee on Intelligence and Security.

(3) A report under subsection (1) must not include personal information (within the meaning of the *Privacy Act 1988*).

Designated reporting period

(4) For the purposes of this section, ***designated reporting period*** means:
  (a) the period beginning at the commencement of this section and ending at the earlier of the following times:
    (i) the end of the 6-month period that began at the commencement of this section;
    (ii) the time when the Parliamentary Joint Committee on Intelligence and Security began to conduct a review under section 60B; or
  (b) the period beginning immediately after the end of the immediately preceding designated reporting period and ending at the earlier of the following times:
    (i) the end of the 6-month period that began immediately after the end of the immediately preceding designated reporting period;
    (ii) the time when the Parliamentary Joint Committee on Intelligence and Security began to conduct a review under section 60B.

60AA Compensation for acquisition of property

(1) If the operation of this Act would result in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from an entity otherwise than on just terms (within the meaning of that paragraph), the Commonwealth is liable to pay a reasonable amount of compensation to the entity.

(2) If the Commonwealth and the entity do not agree on the amount of the compensation, the entity may institute proceedings in:
  (a) the Federal Court of Australia; or

Authorised Version C2022C00160 registered 02/05/2022

(b) the Supreme Court of a State or Territory;

for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

60AB Service of notices, directions and instruments by electronic means

Paragraphs 9(1)(d) and (2)(d) of the *Electronic Transactions Act 1999* do not apply to a notice, direction or instrument under:

(a) this Act; or

(b) the rules; or

(c) the Regulatory Powers Act, so far as that Act relates to this Act.

Note: Paragraphs 9(1)(d) and (2)(d) of the *Electronic Transactions Act 1999* deal with the consent of the recipient of information to the information being given by way of electronic communication.

60A Independent review

(1) The Minister must cause an independent review to be conducted of the operation of this Act.

(2) The review must be conducted after the end of the 12-month period that began at the commencement of this section.

(3) The person or persons who conduct the review must:

(a) give the Minister a written report of the review; and

(b) do so within 12 months after the commencement of the review.

(4) The Minister must cause copies of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the report is given to the Minister.

60B Review of this Act

The Parliamentary Joint Committee on Intelligence and Security may:

Authorised Version C2022C00160 registered 02/05/2022

(a) review the operation, effectiveness and implications of this Act; and
(b) report the Committee's comments and recommendations to each House of the Parliament;

so long as the Committee begins the review before the end of 3 years after the *Security Legislation Amendment (Critical Infrastructure) Act 2021* receives the Royal Assent.

61 Rules

(1) The Minister may, by legislative instrument, makes rules prescribing matters:
  (a) required or permitted by this Act to be prescribed by the rules; or
  (b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) To avoid doubt, the rules may not do the following:
  (a) create an offence or civil penalty;
  (b) provide powers of:
    (i) arrest or detention; or
    (ii) entry, search or seizure;
  (c) impose a tax;
  (d) set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Act;
  (e) directly amend the text of this Act.

Authorised Version C2022C00160 registered 02/05/2022

Endnotes

Endnote 1—About the endnotes

The endnotes provide information about this compilation and the compiled law.

The following endnotes are included in every compilation:

Endnote 1—About the endnotes
Endnote 2—Abbreviation key
Endnote 3—Legislation history
Endnote 4—Amendment history

Abbreviation key—Endnote 2
The abbreviation key sets out abbreviations that may be used in the endnotes.

Legislation history and amendment history—Endnotes 3 and 4
Amending laws are annotated in the legislation history and amendment history.

The legislation history in endnote 3 provides information about each law that has amended (or will amend) the compiled law. The information includes commencement details for amending laws and details of any application, saving or transitional provisions that are not included in this compilation.

The amendment history in endnote 4 provides information about amendments at the provision (generally section or equivalent) level. It also includes information about any provision of the compiled law that has been repealed in accordance with a provision of the law.

Editorial changes
The *Legislation Act 2003* authorises First Parliamentary Counsel to make editorial and presentational changes to a compiled law in preparing a compilation of the law for registration. The changes must not change the effect of the law. Editorial changes take effect from the compilation registration date.

If the compilation includes editorial changes, the endnotes include a brief outline of the changes in general terms. Full details of any changes can be obtained from the Office of Parliamentary Counsel.

Misdescribed amendments
A misdescribed amendment is an amendment that does not accurately describe the amendment to be made. If, despite the misdescription, the amendment can

Authorised Version C2022C00160 registered 02/05/2022

Endnote 1—About the endnotes

be given effect as intended, the amendment is incorporated into the compiled law and the abbreviation "(md)" added to the details of the amendment included in the amendment history.

If a misdescribed amendment cannot be given effect as intended, the abbreviation "(md not incorp)" is added to the details of the amendment included in the amendment history.

Authorised Version C2022C00160 registered 02/05/2022

Endnote 2—Abbreviation key

ad = added or inserted

am = amended

amdt = amendment

c = clause(s)

C[x] = Compilation No. x

Ch = Chapter(s)

def = definition(s)

Dict = Dictionary

disallowed = disallowed by Parliament

Div = Division(s)

ed = editorial change

exp = expires/expired or ceases/ceased to have effect

F = Federal Register of Legislation

gaz = gazette

LA = *Legislation Act 2003*

LIA = *Legislative Instruments Act 2003*

(md) = misdescribed amendment can be given effect

(md not incorp) = misdescribed amendment cannot be given effect

mod = modified/modification

No. = Number(s)

o = order(s)

Ord = Ordinance

orig = original

par = paragraph(s)/subparagraph(s)/sub-subparagraph(s)

pres = present

prev = previous

(prev…) = previously

Pt = Part(s)

r = regulation(s)/rule(s)

reloc = relocated

renum = renumbered

rep = repealed

rs = repealed and substituted

s = section(s)/subsection(s)

Sch = Schedule(s)

Sdiv = Subdivision(s)

SLI = Select Legislative Instrument

SR = Statutory Rules

Sub-Ch = Sub-Chapter(s)

SubPt = Subpart(s)

<u>underlining</u> = whole or part not commenced or to be commenced

Authorised Version C2022C00160 registered 02/05/2022

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Security of Critical Infrastructure Act 2018	29, 2018	11 Apr 2018	11 July 2018 (s 2(1) item 1)	
Foreign Investment Reform (Protecting Australia's National Security) Act 2020	114, 2020	10 Dec 2020	Sch 1 (item 225): 1 Jan 2021 (s 2(1) item 2)	—
Federal Circuit and Family Court of Australia (Consequential Amendments and Transitional Provisions) Act 2021	13, 2021	1 Mar 2021	Sch 2 (item 732): 1 Sept 2021 (s 2(1) item 5)	—
Security Legislation Amendment (Critical Infrastructure) Act 2021	124, 2021	2 Dec 2021	Sch 1 (items 4–73, 75): 3 Dec 2021 (s 2(1) items 2–4)	Sch 1 (items 71, 72)
Security Legislation Amendment (Critical Infrastructure Protection) Act 2022	33, 2022	1 Apr 2022	Sch 1 (items 4–76): 2 Apr 2022 (s 2(1) item 1)	—

Authorised Version C2022C00160 registered 02/05/2022

Endnote 4—Amendment history

Provision affected	How affected
Part 1	
Division 1	
s 3	am No 124, 2021; No 33, 2022
s 4	rs No 124, 2021
	am No 33, 2022
Division 2	
s 5	am No 124, 2021; No 33, 2022
s 6	am No 124, 2021
s 8	am No 33, 2022
s 8D	ad No 124, 2021
s 8E	ad No 124, 2021
s 8F	ad No 124, 2021
s 8G	ad No 124, 2021
	am No 33, 2022
s 9	am No 124, 2021
s 10	am No 124, 2021
s 12	am No 124, 2021; No 33, 2022
s 12A	ad No 124, 2021
s 12B	ad No 124, 2021
s 12C	ad No 124, 2021
s 12D	ad No 124, 2021
s 12E	ad No 124, 2021
s 12F	ad No 124, 2021
	am No 33, 2022
s 12G	ad No 124, 2021
s 12H	ad No 124, 2021
s 12J	ad No 124, 2021
	am No 33, 2022

Authorised Version C2022C00160 registered 02/05/2022

Endnote 4—Amendment history

Provision affected	How affected
s 12K	ad No 124, 2021
	am No 33, 2022
s 12KA	ad No 124, 2021
	am No 33, 2022
s 12L	ad No 124, 2021
	am No 33, 2022
s 12M	ad No 124, 2021
s 12N	ad No 124, 2021
s 12P	ad No 124, 2021
Division 3	
s 13	am No 124, 2021
Part 2	
Division 1	
Division 1 heading	am No 124, 2021
s 18	am No 124, 2021
s 18A	ad No 124, 2021
s 18AA	ad No 124, 2021
	am No 33, 2022
Part 2A	
Part 2A	ad No 33, 2022
s 30AA	ad No 33, 2022
s 30AB	ad No 33, 2022
s 30ABA	ad No 33, 2022
s 30AC	ad No 33, 2022
s 30AD	ad No 33, 2022
s 30AE	ad No 33, 2022
s 30AF	ad No 33, 2022
s 30AG	ad No 33, 2022
s 30AH	ad No 33, 2022
s 30AJ	ad No 33, 2022
s 30AK	ad No 33, 2022

Authorised Version C2022C00160 registered 02/05/2022

Endnote 4—Amendment history

Provision affected	How affected
s 30AKA	ad No 33, 2022
s 30AL	ad No 33, 2022
s 30AM	ad No 33, 2022
s 30AN	ad No 33, 2022
s 30ANA	ad No 33, 2022
s 30ANB	ad No 33, 2022
s 30ANC	ad No 33, 2022
Part 2AA	
Part 2AA	ad No 33, 2022
s 30AP	ad No 33, 2022
s 30AQ	ad No 33, 2022
Part 2B	
Part 2B	ad No 124, 2021
s 30BA	ad No 124, 2021
s 30BB	ad No 124, 2021
s 30BBA	ad No 124, 2021
	am No 33, 2022
s 30BC	ad No 124, 2021
s 30BD	ad No 124, 2021
s 30BE	ad No 124, 2021
	am No 33, 2022
s 30BEA	ad No 124, 2021
s 30BEB	ad No 124, 2021
	am No 33, 2022
s 30BF	ad No 124, 2021
Part 2C	
Part 2C	ad No 33, 2022
Division 1	
s 30CA	ad No 33, 2022

Authorised Version C2022C00160 registered 02/05/2022

Endnote 4—Amendment history

Provision affected	How affected
Division 2	
Subdivision A	
s 30CB	ad No 33, 2022
s 30CC	ad No 33, 2022
Subdivision B	
s 30CD	ad No 33, 2022
s 30CE	ad No 33, 2022
s 30CF	ad No 33, 2022
s 30CG	ad No 33, 2022
s 30CH	ad No 33, 2022
s 30CJ	ad No 33, 2022
s 30CK	ad No 33, 2022
s 30CL	ad No 33, 2022
Division 3	
s 30CM	ad No 33, 2022
s 30CN	ad No 33, 2022
s 30CP	ad No 33, 2022
s 30CQ	ad No 33, 2022
s 30CR	ad No 33, 2022
s 30CS	ad No 33, 2022
s 30CT	ad No 33, 2022
Division 4	
s 30CU	ad No 33, 2022
s 30CV	ad No 33, 2022
s 30CW	ad No 33, 2022
s 30CX	ad No 33, 2022
s 30CY	ad No 33, 2022
s 30CZ	ad No 33, 2022
s 30DA	ad No 33, 2022

Authorised Version C2022C00160 registered 02/05/2022

Endnote 4—Amendment history

Provision affected	How affected
Division 5	
Subdivision A	
s 30DB	ad No 33, 2022
s 30DC	ad No 33, 2022
s 30DD	ad No 33, 2022
s 30DE	ad No 33, 2022
s 30DF	ad No 33, 2022
s 30DG	ad No 33, 2022
s 30DH	ad No 33, 2022
Subdivision B	
s 30DJ	ad No 33, 2022
s 30DK	ad No 33, 2022
s 30DL	ad No 33, 2022
s 30DM	ad No 33, 2022
s 30DN	ad No 33, 2022
s 30DP	ad No 33, 2022
Division 6	
s 30DQ	ad No 33, 2022
Part 3	
Division 2	
s 32	am No 114, 2020; No 124, 2021
s 33	am No 124, 2021
s 35AAA	ad No 33, 2022
s 35AAB	ad No 124, 2021
	am No 33, 2022
Part 3A	
Part 3A	ad No 124, 2021
Division 1	
Division 1	ad No 124, 2021
s 35AA	ad No 124, 2021

Authorised Version C2022C00160 registered 02/05/2022

Endnote 4—Amendment history

Provision affected	How affected
Division 2	
Division 2	ad No 124, 2021
s 35AB	ad No 124, 2021
s 35AC	ad No 124, 2021
s 35AD	ad No 124, 2021
s 35AE	ad No 124, 2021
s 35AF	ad No 124, 2021
s 35AG	ad No 124, 2021
s 35AH	ad No 124, 2021
s 35AJ	ad No 124, 2021
Division 3	
Division 3	ad No 124, 2021
s 35AK	ad No 124, 2021
s 35AL	ad No 124, 2021
s 35AM	ad No 124, 2021
s 35AN	ad No 124, 2021
s 35AP	ad No 124, 2021
Division 4	
Division 4	ad No 124, 2021
s 35AQ	ad No 124, 2021
s 35AR	ad No 124, 2021
s 35AS	ad No 124, 2021
s 35AT	ad No 124, 2021
s 35AU	ad No 33, 2022
s 35AV	ad No 124, 2021
s 35AW	ad No 124, 2021
	am No 33, 2022
Division 5	
Division 5	ad No 124, 2021
s 35AX	ad No 124, 2021
s 35AY	ad No 124, 2021

Authorised Version C2022C00160 registered 02/05/2022

Endnote 4—Amendment history

Provision affected	How affected
s 35AZ	ad No 124, 2021
s 35BA	ad No 124, 2021
s 35BB	ad No 124, 2021
	am No 33, 2022
s 35BC	ad No 124, 2021
s 35BD	ad No 124, 2021
s 35BE	ad No 124, 2021
s 35BF	ad No 124, 2021
s 35BG	ad No 124, 2021
s 35BH	ad No 124, 2021
s 35BJ	ad No 124, 2021
Division 6	
Division 6	ad No 124, 2021
s 35BK	ad No 124, 2021
Part 4	
Division 1	
s 36	am No 124, 2021
Division 3	
Subdivision A	
s 42	am No 124, 2021
s 42A	ad No 33, 2022
s 43AA	ad No 33, 2022
s 43A	ad No 124, 2021
s 43B	ad No 124, 2021
s 43C	ad No 124, 2021
s 43D	ad No 124, 2021
s 43E	ad No 33, 2022
Subdivision B	
s 45	am No 124, 2021
s 46	am No 124, 2021; No 33, 2022
s 47	am No 124, 2021

Authorised Version C2022C00160 registered 02/05/2022

Endnote 4—Amendment history

Provision affected	How affected
Part 5	
Division 1	
s 48	am No 124, 2021
Division 2	
s 49	am No 13, 2021; No 124, 2021
Division 3	
Division 3	ad No 124, 2021
s 49A	ad No 124, 2021
s 49B	ad No 124, 2021
Division 4	
Division 4	ad No 124, 2021
s 49C	ad No 124, 2021
Part 6	
Division 2	
s 51	am No 124, 2021; No 33, 2022
	ed C4
s 51A	ad No 124, 2021
s 52	am No 124, 2021
Part 6A	
Part 6A	ad No 33, 2022
Division 1	
s 52A	ad No 33, 2022
Division 2	
s 52B	ad No 33, 2022
s 52C	ad No 33, 2022
s 52D	ad No 33, 2022
s 52E	ad No 33, 2022
s 52F	ad No 33, 2022
Part 7	
Division 3	
s 59	am No 124, 2021

Authorised Version C2022C00160 registered 02/05/2022

Endnote 4—Amendment history

Provision affected	How affected
Division 4	
Division 4 heading	am No 124, 2021
s 60	am No 124, 2021; No 33, 2022
s 60AAA	ad No 33, 2022
s 60AA	ad No 124, 2021
s 60AB	ad No 124, 2021
s 60A	rs No 33, 2022
s 60B	ad No 124, 2021

Authorised Version C2022C00160 registered 02/05/2022

Endnote 5—Editorial changes

In preparing this compilation for registration, the following kinds of editorial change(s) were made under the *Legislation Act 2003*.

Paragraph 51(1)(d)

Kind of editorial change

Change to spelling

Details of editorial change

Paragraph 51(1)(d) reads as follows:

> (d) there would be a risk to:
> (i) the social or economic stability of Australia or its people; or
> (ii) the defence of Australia; or
> (iii) national security;
> if it were publically known that the asset is a critical infrastructure asset.

This compilation was editorially changed to omit "publically" and substitute "publicly" in paragraph 51(1)(d) to correct the spelling.

Authorised Version C2022C00160 registered 02/05/2022