2022-2023-2024

The Parliament of the Commonwealth of Australia

HOUSE OF REPRESENTATIVES

As passed by both Houses

# **Cyber Security Bill 2024**

No. , 2024

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

# Contents

Part 1-	–Prelimina:	ry	1
	1	Short title	1
	2	Commencement	1
	3	Objects	3
	4	Simplified outline of this Act	4
	5	Extraterritoriality	5
	6	Act binds the Crown	5
	7	Concurrent operation of State and Territory laws	5
	8	Definitions	5
	9	Meaning of cyber security incident	9
	10	Meaning of permitted cyber security purpose	10
	11	Disclosure to State body	11
Part 2–	–Security s	tandards for smart devices	12
Div	ision 1—Pre	liminary	12
	12	Simplified outline of this Part	12
	13	Application of this Part	13
Div	ision 2—Sec	urity standards for relevant connectable	
		oducts	15
	14	Security standards for relevant connectable products	15
	15	Compliance with security standard for a relevant connectable product	15
	16	Obligation to provide and supply products with a statement of compliance with security standard	17
Div	ision 3—Enf	corcement	19
	17	Compliance notice	19
	18	Stop notice	
	19	Recall notice	
	20	Public notification of failure to comply with recall notice	
Div	ision 4—Mis	scellaneous	23
	21	Revocation and variation of notices given under this Part	23
	22	Internal review of decision to give compliance, stop or recall notice	
	23	Examination to assess compliance with security standard and statement of compliance	24
	24	Acquisition of property	26
Part 3–	-Ransomw	are reporting obligations	27

Division	n 1—Pr	eliminary	27
	25	Simplified outline of this Part	27
Division	n 2—Re	porting obligations	28
	26	Application of this Part	28
	27	Obligation to report following a ransomware payment	30
	28	Liability	31
Division	n 3—Pr	otection of information	32
	29	Ransomware payment reports may only be used or disclosed for permitted purposes	32
	30	Limitations on secondary use and disclosure of information in ransomware payment reports	33
	31	Legal professional privilege	36
	32	Admissibility of information in ransomware payment report against reporting business entity	37
Part 4—Co	ordina	tion of significant cyber security incidents	39
Division	n 1—Pr	eliminary	39
21,15101	33	Simplified outline of this Part	
	34	Meaning of significant cyber security incident	
Division	n 2—Vo	oluntary information sharing with the National	
Division		ber Security Coordinator	40
	35	Impacted entity may voluntarily provide information to National Cyber Security Coordinator in relation to a significant cyber security incident	40
	36	Voluntary provision of information in relation to other incidents or cyber security incidents	
	37	Role of the National Cyber Security Coordinator	
Division	n 3—Pr	otection of information	43
	38	Information provided in relation to a significant cyber security incident—use and disclosure by National Cyber Security Coordinator	42
	39	Information provided in relation to other incidents—use and disclosure by National Cyber Security Coordinator	
	40	Limitations on secondary use and disclosure	
	41	Legal professional privilege	
	42	Admissibility of information voluntarily given by impacted entity	
	43	National Cyber Security Coordinator not compellable as witness	
Division	n 4—Mi	iscellaneous	52

	44	Interaction with other requirements to provide information in	
		relation to a cyber security incident	52
Part 5—C	yber In	cident Review Board	53
Divisio	on 1—Pr	eliminary	53
	45	Simplified outline of this Part	53
Divisio	on 2—Re		54
211151	46	Board must cause reviews to be conducted	
	47	Board may discontinue a review	
	48	Chair may request information or documents	
	49	Chair may require certain entities to produce documents	
	50	Civil penalty—failing to comply with a notice to produce documents	
	51	Draft review reports	
	52	Final review reports	
	53	Certain information must be redacted from final review reports	60
	54	Protected review reports	61
Divisio	on 3—Pr	otection of information relating to reviews	62
	55	Limitations on use and disclosure by the Board	62
	56	Limitations on secondary use and disclosure	63
	57	Legal professional privilege	
	58	Admissibility of information given by an entity that has been requested or required by the Board	67
	59	Disclosure of draft review reports prohibited	68
Divisio	on 4—Es	tablishment, functions and powers of the Board	69
	60	Cyber Incident Review Board	69
	61	Constitution of the Board	69
	62	Functions of the Board	69
	63	Independence	70
Divisio	on 5—Te	erms and conditions of appointment of the Chair	
	an	nd members of the Board	72
	64	Appointment of Chair	72
	65	Remuneration of the Chair	72
	66	Appointment of standing members of the Board	72
	67	Remuneration of standing members of the Board	73
	68	Acting Chair	73
	69	Terms and conditions etc. for standing members	74
Divisio	on 6—Ex	pert Panel, staff assisting and consultants	75
	70	Expert Panel	75

	71	Arrangements relating to staff of the Department	75
	72	Consultants	76
Division 7-	—Oth	er matters relating to the Board	77
	73	Board procedures	77
	74	Liability	77
	75	Certification of involvement in review	78
	76	Annual report	79
	77	Rules may prescribe reporting requirements etc	79
Part 6—Regu	lator	y powers	80
Division 1-	—Pre	liminary	80
	78	Simplified outline of this Part	80
Division 2	—Civi	il penalty provisions, enforceable undertakings	
	and	injunctions	81
	79	Civil penalty provisions, enforceable undertakings and injunctions	81
Division 3	-Moi	nitoring and investigation powers	84
	80	Monitoring powers	84
	81	Investigation powers	86
Division 4	—Infr	ringement notices	89
	82	Infringement notices	89
Division 5	—Oth	er matters	91
	83	Contravening a civil penalty provision	91
Part 7—Misc	ellane	eous	92
	84	Simplified outline of this Part	92
	85	How this Act applies in relation to non-legal persons	92
	86	Delegation by Secretary	93
	87	Rules	94
	88	Review of this Act	95

Austra	llians, and for other purposes
The Par	rliament of Australia enacts:
Part 1-	—Preliminary
1 Short t	title
	This Act is the <i>Cyber Security Act 2024</i> .
2 Comm	nencement
(1	Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with

Cyber Security Bill 2024

A Bill for an Act relating to cyber security for

1

No. , 2024

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

Commencement in	nformation	
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. Part 1 and anything in this Act not elsewhere covered by this table	The day after this Act receives the Royal Assent.	
2. Part 2	A single day to be fixed by Proclamation.	
	However, if the provisions do not commence within the period of 12 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	
3. Part 3	A single day to be fixed by Proclamation.	
	However, if the provisions do not commence within the period of 6 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	
4. Part 4	The day after this Act receives the Royal Assent.	
5. Part 5	A single day to be fixed by Proclamation.	
	However, if the provisions do not commence within the period of 6 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	
6. Parts 6 and 7	The day after this Act receives the Royal Assent.	
Note:	This table relates only to the provisions of this A enacted. It will not be amended to deal with any this Act.	

4 5 6

1 2 3	(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.
4	3 Objects	
5		The objects of this Act are to:
6		(a) improve the cyber security of products that:
7		(i) can connect directly or indirectly to the internet; and
8		(ii) will be acquired in Australia;
9 10		by requiring manufacturers and suppliers of those products to comply with security standards specified in the rules; and
11		(b) encourage the provision of information relating to the
12		provision of payments or benefits (called ransomware
13		payments) to entities seeking to benefit from cyber security
14		incidents by imposing reporting obligations on entities in
15		relation to the payment of such payments or benefits; and
16		(c) facilitate the whole of Government response to significant
17		cyber security incidents by providing for the National Cyber
18 19		Security Coordinator to lead across the whole of Government the coordination and triaging of action in response to
20		significant cyber security incidents; and
21		(d) prevent, improve the detection of, improve the response to
22		and minimise the impact of cyber security incidents by
23		establishing the Cyber Incident Review Board to:
24		(i) cause reviews to be conducted in relation to certain
25		cyber security incidents; and
26		(ii) make recommendations to government and industry
27		about actions that could be taken to prevent, detect,
28		respond to or minimise the impact of, incidents of a
29		similar nature in the future; and
30		(e) improve the response to and minimise the impact of cyber
31		security incidents (including imminent incidents) through
32		encouraging entities impacted, or probably impacted, by such
33		cyber security incidents to provide information to the
34		Australian Government about the incidents by ensuring that:
35		(i) the information provided is only used and disclosed for
36		limited purposes; and

2.5

(ii) the information provided is not admissible in evidence
in proceedings against the entities that provided the
information; and
(f) to facilitate the sharing of information about cyber security
incidents with State and Territory Governments for limited
purposes, with their consent that the information is only to be
used and disclosed for limited purposes.

#### 4 Simplified outline of this Act

This Act provides for mandatory security standards for certain products that can directly or indirectly connect to the internet (called relevant connectable products).

This Act also provides an obligation to report payments or benefits (called ransomware payments) provided to an entity that is seeking to benefit from a cyber security incident.

Information may be voluntarily provided to the National Cyber Security Coordinator in relation to a significant cyber security incident. The National Cyber Security Coordinator's role is to lead across the whole of Government the coordination and triaging of action in response to a significant cyber security incident.

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

Information provided by entities under provisions of this Act may only be used and disclosed for limited purposes. Certain information provided to the Australian Government under this Act is not admissible in evidence in proceedings against the entity that provided the information.

, 2024

No.

	This Act also deals with administrative matters such as delegations and the power to make rules.  Tritoriality  This Act applies both within and outside Australia.  Note: This Act extends to every external Territory.
	This Act applies both within and outside Australia.  Note: This Act extends to every external Territory.
act bind	Note: This Act extends to every external Territory.
act bind	
ct bind	ls the Crown
	ls 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.
	Note: The Crown (other than a Crown authority) is not liable to a pecuniary penalty for the breach of a civil penalty provision or to be given an infringement notice: see subsections 79(8) and 82(7).
(3)	The protection in subsection (2) does not apply to an authority of the Crown.
Concuri	rent 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.
) Pefinition	ons
	In this Act:
	ASD means the Australian Signals Directorate.
	benefit includes any advantage and is not limited to property.
	business has the same meaning as in the Income Tax Assessment Act 1997.

1	Chair means the Chair of the Cyber Incident Review Board.
2	civil penalty provision has the same meaning as in the Regulatory
3	Powers Act.
4	Commonwealth body means:
5	(a) a Minister of the Commonwealth; or
6	(b) a Department of State of the Commonwealth; or
7	(c) a body (whether incorporated or not) that:
8	(i) is established, or continued in existence, for a public
9	purpose by or under a law of the Commonwealth; and
10	(ii) is not an authority of the Crown.
11	Commonwealth enforcement body means:
12	(a) the Australian Federal Police; or
13	(b) the Australian Prudential Regulation Authority; or
14	(c) the Australian Securities and Investments Commission; or
15	(d) the Inspector of the National Anti-Corruption Commission;
16	or
17	(e) the Office of the Director of Public Prosecutions; or
18	(f) the National Anti-Corruption Commissioner; or
19	(g) Sport Integrity Australia; or
20	(h) another Commonwealth body, to the extent that it is
21	responsible for administering, or performing a function
22	under, a law that imposes a penalty or sanction for a criminal
23	offence.
24	Commonwealth officer has the same meaning as in Part 5.6 of the
25	Criminal Code.
26	computer has the same meaning as in the Security of Critical
27	Infrastructure Act 2018.
28	coronial inquiry means a coronial inquiry, coronial investigation
29	or coronial inquest under a law of the Commonwealth, or of a State
30	or Territory.
31	critical infrastructure asset has the same meaning as in the
32	Security of Critical Infrastructure Act 2018.

1 2	<i>Cyber Incident Review Board</i> or <i>Board</i> means the Cyber Incident Review Board established by section 60.
3	cyber security incident has the meaning given by section 9.
4	designated Commonwealth body means:
5	(a) a Department, or a body established by a law of the
6	Commonwealth, specified in the rules; or
7	(b) if no rules are made for the purposes of paragraph (a)—the
8	Department and ASD.
9	draft review report has the meaning given by subsection 51(1).
10	entity means any of the following:
11	(a) an individual;
12	(b) a body corporate;
13	(c) a partnership;
14	(d) an unincorporated association that has a governing body;
15	(e) a trust;
16	(f) an entity that is a responsible entity for a critical
17	infrastructure asset.
18	Expert Panel means the Expert Panel established by the Board
19	under section 70.
20	<i>final review report</i> has the meaning given by subsection 52(1).
21	intelligence agency means:
22	(a) the agency known as the Australian Criminal Intelligence
23	Commission established by the <i>Australian Crime</i>
24	Commission Act 2002; or
25	(b) the Australian Geospatial-Intelligence Organisation; or
26	(c) the Australian Secret Intelligence Service; or
27	(d) the Australian Security Intelligence Organisation; or
28	(e) ASD; or
29	(f) the Defence Intelligence Organisation; or
30	(g) the Office of National Intelligence.

1 2	<i>internet-connectable product</i> has the meaning given by subsection 13(4).
3 4	<i>manufacturer</i> has the same meaning as in the Australian Consumer Law.
5	National Cyber Security Coordinator means:
6 7	(a) the officer of the Department known as the National Cyber Security Coordinator; and
8	(b) the APS employees, and officers or employees of
9	Commonwealth bodies, whose services are made available to
10	the officer in connection with the performance of any of the
11	officer's functions or the exercise of any of the officer's
12	powers under this Act.
13	network-connectable product has the meaning given by
14	subsection 13(5).
15	permitted cyber security purpose for a cyber security incident has
16	the meaning given by section 10.
17 18	<i>personal information</i> has the same meaning as in the <i>Privacy Act</i> 1988.
19	protected review report has the meaning given by subsection 54(1)
20	ransomware payment has the meaning given by subsection 26(1).
21	ransomware payment report means a report given by an entity
22	under subsection 27(1).
23	Regulatory Powers Act means the Regulatory Powers (Standard
24	Provisions) Act 2014.
25	relevant connectable product has the meaning given by
26	subsection 13(2).
27	reporting business entity has the meaning given by
28	subsection 26(2).
29	responsible entity, for an asset, has the same meaning as in the
30	Security of Critical Infrastructure Act 2018.

Secretary means the Secretary of the Department.
sensitive information has the same meaning as in the <i>Privacy Act</i> 1988.
<i>sensitive review information</i> has the meaning given by subsection 53(2).
<i>significant cyber security incident</i> has the meaning given by section 34.
<ul> <li>(a) a Minister of a State or Territory; or</li> <li>(b) a Department of State of a State or Territory or a Department of the Public Service of a State or Territory; or</li> <li>(c) a body (whether incorporated or not) that: <ul> <li>(i) is established, or continued in existence, for a public purpose by or under a law of a State or Territory; and</li> <li>(ii) is not an authority of the Crown.</li> </ul> </li> </ul>
<i>supply</i> has the same meaning as in the Australian Consumer Law and <i>supplied</i> and <i>supplier</i> have corresponding meanings.
9 Meaning of cyber security incident
<ul> <li>(1) A cyber security incident is one or more acts, events or circumstances:</li> <li>(a) of a kind covered by the meaning of cyber security incident in the Security of Critical Infrastructure Act 2018; or</li> <li>(b) involving unauthorised impairment of electronic communication to or from a computer, within the meaning of that phrase in that Act, but as if that phrase did not exclude the mere interception of any such communication.</li> </ul>
<ul> <li>(2) However, an incident is only a <i>cyber security incident</i> for the purposes of this Act if:</li> <li>(a) the incident involves a critical infrastructure asset; or</li> <li>(b) the incident involves the activities of an entity that is a corporation to which paragraph 51(xx) of the Constitution applies; or</li> </ul>

1	(c)	the incident is or was effected by means of a telegraphic,
2		telephonic or other like service within the meaning of
3		paragraph 51(v) of the Constitution (including, for example, by means of the internet); or
	(4)	the incident is impeding or impairing, or has impeded or
5 6	(u)	impaired, the ability of a computer to connect to such a
7		service; or
8	(e)	the incident has seriously prejudiced or is seriously
9	(0)	prejudicing:
10		(i) the social or economic stability of Australia or its
11		people; or
12		(ii) the defence of Australia; or
13		(iii) national security.
14	10 Meaning of	permitted cyber security purpose
15		of the following is a <i>permitted cyber security purpose</i> for a
16		r security incident:
17		the performance of the functions of a Commonwealth body
18	(4)	(to the extent that it is not a Commonwealth enforcement
19		body) relating to responding to, mitigating or resolving the
20		cyber security incident;
21	(b)	the performance of the functions of a State body relating to
22		responding to, mitigating or resolving the cyber security
23		incident;
24	(c)	the performance of the functions of the National Cyber
25		Security Coordinator under Part 4 relating to the cyber
26		security incident;
27	(d)	informing and advising the Minister, and other Ministers of
28		the Commonwealth, about the cyber security incident;
29	(e)	preventing or mitigating material risks that the cyber security
30 31		incident has seriously prejudiced, is seriously prejudicing, or could reasonably be expected to prejudice:
32		(i) the social or economic stability of Australia or its
33		people; or
34		(ii) the defence of Australia; or
35		(iii) national security;
		× /

1	(f) preventing or mitigating material risks to a critical
2	infrastructure asset;
3	(g) the performance of the functions of an intelligence agency;
4	(h) the performance of the functions of a Commonwealth
5	enforcement body.
6	Note 1: There are some limitations in relation to civil or regulatory functions
7	against entities that have provided information in relation to the
8	incident: see subsections 38(2) and 39(3).
9	Note 2: Certain information must not be disclosed to a State body under Parts
10	of this Act unless a Minister of the State or Territory has consented to
11	those Parts applying to the State body: see section 11.
12	11 Disclosure to State body
13	(1) Despite any other provision of this Act, information that may be
14	disclosed to a State body under Part 3, 4 or 5 must not be disclosed
15	to the State body under that Part unless:
16	(a) a Minister of the State or Territory has informed the Minister
17	administering this Act, in writing, that the State or Territory
18	gives consent to the provisions of that Part applying to the
19	State body; and
20	(b) a Minister of the State or Territory has not informed the
21	Minister administering this Act, in writing, that the State or
22	Territory withdraws that consent.
23	(2) For the purposes of paragraph (1)(a), a Minister of a State or
24	Territory may give consent in relation to all State bodies, a class of
25	State bodies, or particular State bodies, of that State or Territory.

1

3

29

## Part 2—Security standards for smart devices

#### 2 Division 1—Preliminary

#### 12 Simplified outline of this Part

The rules may provide mandatory security standards for products 4 5 that can directly or indirectly connect to the internet (called relevant connectable products) that will be acquired in Australia in 6 specified circumstances. 7 If the rules provide a security standard for a product: 8 manufacturers must manufacture the product in 9 compliance with the requirements of the security 10 standard if they are aware, or could reasonably be 11 expected to be aware, that the product will be acquired 12 in Australia in the specified circumstances; and 13 (b) those manufacturers must also comply with any other 14 obligations relating to the product in the security 15 standard (for example, obligations to publish 16 information about the product); and 17 (c) if the product does not comply it must not be supplied in 18 Australia if the supplier is aware, or could reasonably be 19 expected to be aware, that the products will be acquired 20 in Australia in those specified circumstances; and 21 those suppliers must supply the product in Australia 22 accompanied by a statement of compliance. 23 A compliance notice, a stop notice and a recall notice may be given 24 for non-compliance with obligations in this Part. Internal review 25 may be sought for a decision to issue a notice. 26 An independent audit of a product may be undertaken to determine 27 compliance with the requirements of a security standard or 28

requirements for the statement of compliance. The Secretary may

request the manufacturer or supplier to provide the product, the

statement of compliance or both for the purposes of the audit. 13 Application of this Part 3 (1) This Part applies to a relevant connectable product that is: 4 (a) manufactured on or after the commencement of this Part; or 5 (b) supplied (other than as second hand goods) on or after the 6 commencement of this Part. 7 (2) A *relevant connectable product* is a product that: 8 (a) is an internet-connectable product or a network-connectable 9 product; and 10 (b) is not exempted under the rules. 11 (3) For the purposes of paragraph (2)(b), the rules may specify that: 12 (a) classes of products are exempted; or 13 (b) particular products are exempted. 14 (4) An *internet-connectable product* is a product that is capable of 15 connecting to the internet using a communication protocol that 16 forms part of the internet protocol suite to send and receive data 17 over the internet. 18 (5) A *network-connectable product* is a product that: 19 (a) is capable of both sending and receiving data by means of a 20 transmission involving electrical or electromagnetic energy; 21 and 22 (b) is not an internet-connectable product; and 23 (c) meets the condition in subsection (6) or (7). 24 (6) A product meets the condition in this subsection if it is capable of 25 connecting directly to an internet-connectable product by means of 26 a communication protocol that forms part of the internet protocol 2.7 suite. 28 (7) Subject to subsections (8) and (9), a product meets the condition in 29 this subsection if: 30

1

2

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

# Division 2—Security standards for relevant connectable products

2	products
3	14 Security standards for relevant connectable products
4	(1) The rules may make provision for, or in relation to, security
5 6	standards for specified classes of relevant connectable products that will be acquired in Australia in specified circumstances.
7	(2) Without limiting subsection (1) a class of relevant connectable
8	products specified for the purposes of that subsection may consist
9 10	of a particular relevant connectable product or of all relevant connectable products.
11	(3) Despite subsection 14(2) of the Legislation Act 2003, the rules may
12	make provision in relation to a matter by applying, adopting or
13	incorporating, with or without modification, any matter contained
14	in an instrument or other writing as in force or existing from time
15	to time.
16	15 Compliance with security standard for a relevant connectable
17	product
18	Manufacturer must comply
19	(1) An entity must manufacture a relevant connectable product in
20	compliance with the requirements of the security standard for a
21	class of relevant connectable product that will be acquired in
22	Australia in specified circumstances if:
23	(a) the product is included in that class; and
24	(b) the entity is aware, or could reasonably be expected to be
25	aware, that the product will be acquired in Australia in those
26	circumstances.
27	(2) The entity must comply with any other requirements of the security
28	standard that apply to the manufacturer of a product included in
29	that class.

1	(3) An entity must not supply a product in Australia that was not
2	manufactured in compliance with the requirements of the security
3	standard for a class of relevant connectable product that will be acquired in Australia in specified circumstances if:
4	
5	(a) the product is included in that class; and
6	(b) the entity is aware, or could reasonably be expected to be
7 8	aware, that the product will be acquired in Australia in those circumstances.
9	(4) The entity must comply with any other requirements of the security
10	standard that apply to the supplier of a product included in that
11	class.
12	Exception
13	(5) However, to the extent that a requirement in the security standard
14	does not relate to any of the matters in subsection (6), an entity is
15	not required to comply with subsections (1) to (4) if the entity is
16	not:
17	(a) an entity that is a corporation to which paragraph $51(xx)$ of
18	the Constitution applies; or
19	(b) an entity that is undertaking activities in the course of, or in
20	relation to, trade or commerce with other countries, among
21	the States, between Territories or between a Territory and a
22	State.
23	(6) The matters are the following:
24	(a) the direct, or indirect, connection of the relevant connectable
25	product to, a telegraphic, telephonic or other like service
26	within the meaning of paragraph 51(v) of the Constitution
27	(including, for example, connection to the internet);
28	(b) the direct, or indirect, use by the relevant connectable product
29	of such a service (including, for example, use of the internet);
30	(c) measures that would protect the relevant connectable product
31	from an attack effected by means of such a service
32	(including, for example, by means of the internet).

No. , 2024

16

1	to Obligat	tion to provide and supply products with a statement of
2		compliance with security standard
3		Manufacturer must provide statement of compliance
4	(1)	An entity that manufactures a relevant connectable product must
5		provide, for the supply of the product in Australia, a statement of
6		compliance with the security standard for a class of relevant
7		connectable product that will be acquired in Australia in specified
8		circumstances if:
9		(a) the product is included in that class; and
0		(b) the entity is aware, or could reasonably be expected to be
1		aware, that the product will be acquired in Australia in those
12		circumstances.
13	(2)	The entity must retain a copy of the statement of compliance for
4	,	the period specified in the rules for that class of statements.
15		Supplier must supply the product with statement of compliance
6	(3)	An entity that supplies a relevant connectable product in Australia
17	. ,	must supply the product with a statement of compliance with the
8		security standard for a class of relevant connectable product that
9		will be acquired in Australia in specified circumstances if:
20		(a) the product is included in that class; and
21		(b) the entity is aware, or could reasonably be expected to be
22		aware, that the product will be acquired in Australia in those
23		circumstances.
24	(4)	The entity must retain a copy of the statement of compliance for
25		the period specified in the rules for that class of statements.
26		Requirements for statement of compliance
27	(5)	The statement of compliance with the security standard under
28		subsection (1) or (2) must meet the requirements provided by the
29		rules for that class of statements.

1

2

3

4

5

Matters	relating	to the	rule	making	nowers
Muncis	reiming	io inc	, i uic	making	powers

(6) Without limiting subsection (2), (4) or (5) a class of statements may consist of a statement for a particular relevant connectable product or a particular security standard or all relevant connectable products or all security standards.

## **Division 3—Enforcement**

2	17 Compliance	notice
3	(1) The S	Secretary may give an entity that must comply with an
4	•	ation under section 15 or 16 a compliance notice if the
5	Secre	tary:
6 7	(a)	is reasonably satisfied that the entity is not complying with the obligation; or
8	(b)	is aware of information that suggests that the entity may not
9		be complying with the obligation.
10	(2) The c	compliance notice must:
11	(a)	set out the name of the entity to which the notice is given;
12		and
13	(b)	set out brief details of the non-compliance or possible
14		non-compliance; and
15	(c)	specify action within the entity's control that the entity must
16		take in order to address the non-compliance or possible
17		non-compliance; and
18	(d)	specify a reasonable period within which the entity must take
19		the specified action; and
20	(e)	if the Secretary considers it appropriate—specify a
21		reasonable period within which the entity must provide the
22		Secretary with evidence that the entity has taken the specified
23	(6)	action; and
24	(1)	explain what may happen if the entity does not comply with
25		the notice; and
26	(g)	explain how the entity may seek review of the decision to
27	4.	issue the notice; and
28	(h)	set out any other matters prescribed by the rules.
29		re giving the notice to the entity, the Secretary must:
30	(a)	notify the entity that the Secretary intends to give the notice
31		to the entity; and

1 2 3	(b	) give the entity a specified period (which must not be shorter than 10 days) to make representations about the giving of the notice.
4 5	a pa	y one compliance notice may be given to an entity in relation to articular instance of the entity's non-compliance, or possible
6	non	-compliance, with an obligation under section 15 or 16.
7	18 Stop notice	
8		Secretary may give an entity that must comply with an
9	obli	gation under section 15 or 16 a stop notice if:
10 11	(a	) the entity has been given a compliance notice under section 17 in relation to the non-compliance with the
12		obligation; and
13	(b	) the Secretary is reasonably satisfied that:
14	·	(i) the entity has not complied with the compliance notice;
15		or
16		(ii) actions taken by the entity to rectify non-compliance
17		with the obligation (whether in accordance with the
18		compliance notice or otherwise) are inadequate to
19		rectify the non-compliance.
20	(2) The	e stop notice must:
21	(a	) set out the name of the entity to which the notice is given;
22		and
23	(b	) set out brief details of the non-compliance; and
24	(c	) specify action within the entity's control that the entity must
25		take, or refrain from taking, in order to address the
26		non-compliance; and
27	(d	) specify a reasonable period within which the entity must take
28		the specified action or refrain from taking the specified
29	(-	action; and
30	(e	) if the Secretary considers it appropriate—specify a reasonable period within which the entity must provide the
31 32		Secretary with evidence that the entity has taken the specified
33		action or refrained from taking the specified action; and
34	(f	explain what may happen if the entity does not comply with
35		the notice; and

1 2	<ul><li>(g) explain how the entity may seek review of the decision to issue the notice; and</li></ul>
3	(h) set out any other matters prescribed by the rules.
4	(3) Before giving the notice to the entity, the Secretary must:
5	(a) notify the entity that the Secretary intends to give the notice
6	to the entity; and
7	(b) give the entity a specified period (which must not be shorter
8	than 10 days) to make representations about the giving of the
9	notice.
10	(4) Only one stop notice may be given to an entity in relation to a
11	particular instance of the entity's non-compliance with an
12	obligation under section 15 or 16.
13	19 Recall notice
14	(1) The Secretary may give an entity that must comply with an
15	obligation under section 15 or 16 a recall notice if:
16	(a) the entity has been given a stop notice under section 18 in
17	relation to the non-compliance with the obligation; and
18	(b) the Secretary is reasonably satisfied that:
19	(i) the entity has not complied with the stop notice; or
20	(ii) actions taken by the entity to rectify the non-compliance
21	with the obligation (whether in accordance with the
22	compliance notice or otherwise) are inadequate to
23	rectify the non-compliance.
24	(2) The recall notice must:
25	(a) set out the name of the entity to which the notice is given;
26	and
27	(b) set out brief details of the non-compliance; and
28	(c) specify action that the entity must take to do any or all of the
29	following:
30	(i) ensure, to the extent within the entity's control, the
31	product is not acquired in Australia;
32	(ii) ensure, to the extent within the entity's control, that the
33	product is not supplied to suppliers for supply in Australia;
34	Australia,
	-

1		(iii) arrange for the return, within a specified reasonable
2		period, of the product to the entity, or if the entity is not
3		the manufacturer of the product, the manufacturer of the
4	(1)	product; and
5		specify a reasonable period within which the entity must take
6		the specified action; and
7		if the Secretary considers it appropriate—specify a
8		reasonable period within which the entity must provide the
9 10		Secretary with evidence that the entity has taken the specified action; and
		explain what may happen if the entity does not comply with
11 12		the notice; and
13	(g)	explain how the entity may seek review of the decision to
14		issue the notice; and
15	(h)	set out any other matters prescribed by the rules.
16	(3) Before	e giving the notice to the entity, the Secretary must:
17	(a) 1	notify the entity that the Secretary intends to give the notice
18	1	to the entity; and
19		give the entity a specified period (which must not be shorter
20		than 10 days) to make representations about the giving of the
21	1	notice.
22		one recall notice may be given to an entity in relation to a
23	_	ular instance of the entity's non-compliance with an
24	obliga	tion under section 15 or 16.
25	20 Public notifie	cation of failure to comply with recall notice
26	If an e	entity fails to comply with a recall notice, the Minister may
27	publis	h the following information on the Department's website, or
28	in any	other way the Minister considers appropriate:
29	(a)	the identity of the entity;
30	(b)	details of the product;
31	(c)	details of the non-compliance;
32	(d) 1	risks posed by the product relating to the non-compliance;
33		any other matters prescribed by the rules.
	(-)	J

22

# **Division 4—Miscellaneous**

2

### 21 Revocation and variation of notices given under this Part

3	Variation
4	(1) The Secretary may, by notice in writing given to an entity, vary a
5	compliance notice, stop notice or recall notice given under this Part
6	to the entity if the Secretary is reasonably satisfied that the
7	variation is required:
8	(a) in order to rectify an error, defect or ambiguity in the notice;
9	or
10	(b) to adequately rectify the non-compliance, or possible
11	non-compliance, to which the notice relates.
12	(2) Before giving the notice to the entity under subsection (1), the
13	Secretary must:
14	(a) notify the entity that the Secretary intends to give the notice
15	to the entity; and
16	(b) give the entity a specified period (which must not be shorter
17	than 10 days) to make representations about the giving of the
18	notice.
19	(3) A varied compliance notice, stop notice or recall notice has the
20	same effect as the original notice for the purposes of this Part.
21	Revocation
22	(4) The Secretary may, by notice in writing given to an entity, revoke a
23	compliance notice, stop notice or recall notice given under this Part
24	to the entity if the Secretary is no longer satisfied that the grounds
25	for issuing the notice were met.
26	(5) If a compliance notice, stop notice or recall notice, relating to
27	non-compliance or possible non-compliance by an entity with an
28	obligation, is revoked under subsection (4), no further notices may
29	be issued under this Part in relation to that non-compliance.

1 2	22 Internal review of decision to give compliance, stop or recall notice
3	(1) An entity may apply, in writing, to the Secretary for review (an <i>internal review</i> ) of a decision:
5	(a) to give the entity a compliance notice under section 17; or
6	(b) to give the entity a stop notice under section 18; or
7	(c) to give the entity a recall notice under section 19; or
8	(d) to vary, under section 21, a notice given to the entity.
9 10	(2) An application for an internal review must be made within 30 days after the day on which the notice was given to the entity.
11	(3) The decision-maker for the internal review is:
12	(a) the Secretary; or
13	(b) if the Secretary made the decision personally—a person:
14	(i) to whom the power to issue a notice of that kind has
15	been delegated under section 86; and
16 17	<ul><li>(ii) that was not involved in the making of the Secretary's decision.</li></ul>
18	(4) Within 30 days after the application is received, the decision-maker
19	must:
20	(a) review the decision; and
21	(b) affirm, vary or revoke the decision; and
22 23	(c) if the decision is revoked—make such other decision (if any) that the decision-maker thinks appropriate.
24	(5) The decision-maker for the reviewable decision must, as soon as
25	practicable after making a decision under subsection (4), give the
26	applicant a written statement of the decision-maker's reasons for
27	the decision.
28 29	23 Examination to assess compliance with security standard and statement of compliance
30 31 32	(1) If an entity must comply with an obligation in section 15 or 16 in relation to a relevant connectable product, the Secretary may engage an appropriately qualified and experienced expert to carry
	6.6

1 2	out an independent examination of the product to determine either or both of the following:
3	(a) whether the product complies with the security standard for
4	the class of relevant connectable product;
5	(b) whether the statement of compliance for the product
6	complies with the requirements of section 16.
7	(2) The expert may examine the product, for example, by doing any of
8	the following:
9	(a) opening any package in which the product is contained;
10	(b) operating the product;
11	<ul> <li>(c) testing or analysing the product, including through the use of electronic equipment;</li> </ul>
13	(d) if the product contains a record or document—reading the
14	record or document either directly or with the use of an
15	electronic device;
16	(e) taking photographs or video recordings of the product.
17	Request for product and statement of compliance
18	(3) For the purposes of the examination, the Secretary may request, by
19	notice in writing, the entity to provide the product, or the statement
20	of compliance for the product, or both.
21	(4) The notice must:
22	(a) specify the product; and
23	(b) if the entity is not the manufacturer—specify the
24	manufacturer of the product (if known); and
25	(c) specify a reasonable period within which the entity must
26	provide the notice; and
27	(d) specify the period for which the product will be retained for
28	testing; and
29	(e) specify the requirements of the security standard that the
80	product will be tested against; and
31	(f) explain the kind of testing or analysis that will be done; and
32	(g) explain what may happen if:
33	(i) the entity does not comply with the notice; or

1 2	(ii) the entity does not comply with its obligations in section 15 or 16 in relation to the product; and
3	(h) set out any other matters prescribed by the rules.
4	Compensation
5 6	(5) An entity is entitled to be paid by the Commonwealth reasonable compensation for complying with a request under subsection (3).
7	24 Acquisition of property
,	24 Acquisition of property
8	This Part has no effect to the extent (if any) that its operation
9	would result in an acquisition of property (within the meaning of
10	paragraph 51(xxxi) of the Constitution) from a person otherwise
11	than on just terms (within the meaning of that paragraph).

## Part 3—Ransomware reporting obligations

#### 2 Division 1—Preliminary

1

3

#### 25 Simplified outline of this Part

This Part imposes reporting obligations on certain entities who are 4 5 impacted by a cyber security incident, and who have provided or are aware that another entity has provided, a payment or benefit 6 7 (called a ransomware payment) to an entity that is seeking to benefit from the impact or the cyber security incident. Particular information must be included in a ransomware payment 9 report, including information relating to the cyber security incident, 10 the demand made by the extorting entity and the ransomware 11 payment. 12 An entity may be liable to a civil penalty if the entity fails to make 13 a ransomware payment report as required by this Part. 14

1

# **Division 2—Reporting obligations**

2	26 Application of this Part
3	(1) This Part applies if:
4	(a) an incident has occurred, is occurring or is imminent; and
5	(b) the incident is a cyber security incident; and
6	(c) the incident has had, is having, or could reasonably be
7	expected to have, a direct or indirect impact on a reporting
8	business entity; and
9	(d) an entity (the extorting entity) makes a demand of the
10	reporting business entity, or any other entity, in order to
11	benefit from the incident or the impact on the reporting
12	business entity; and
13	(e) the reporting business entity provides, or is aware that
14	another entity has provided on their behalf, a payment or
15	benefit (a <i>ransomware payment</i> ) to the extorting entity that
16	is directly related to the demand.
17	(2) An entity is a <i>reporting business entity</i> if, at the time the
18	ransomware payment is made:
19	(a) the entity:
20	(i) is carrying on a business in Australia with an annual
21	turnover for the previous financial year that exceeds the
22	turnover threshold for that year; and
23	(ii) is not a Commonwealth body or a State body; and
24	(iii) is not a responsible entity for a critical infrastructure
25	asset; or
26	(b) the entity is a responsible entity for a critical infrastructure
27	asset to which Part 2B of the Security of Critical
28	Infrastructure Act 2018 applies.
29	(3) For the purposes of subparagraph (2)(a)(i), the turnover threshold
30	is:
31	(a) if a business has been carried on for only part of the previous
32	financial year—the amount worked out in the manner
33	prescribed by the rules; or

1 2	(b) in any other case—the amount prescribed by, or worked out in the manner prescribed by, the rules.
_	in the manner presentate by, the renes.
3	Presumption
4	(4) For the purposes of paragraph (1)(b), an incident (other than an
5	incident covered by paragraph 9(2)(a) or (b)) is presumed to be a
6	cyber security incident if:
7	(a) the incident was probably effected, is probably being effected
8	or could reasonably be expected to be effected, by means of a
9	telegraphic, telephonic or other like service within the
10	meaning of paragraph 51(v) of the Constitution (including,
11	for example, by means of the internet); or
12	(b) the incident has probably impeded or impaired, or is probably
13	impeding or impairing or could reasonably be expected to impede or impair, the ability of a computer to connect to such
14 15	a service; or
	·
16 17	(c) the incident has probably seriously prejudiced, is probably seriously prejudicing, or could reasonably be expected to
18	prejudice:
19	(i) the social or economic stability of Australia or its
20	people; or
21	(ii) the defence of Australia; or
22	(iii) national security.
23	Note: Paragraphs 9(2)(a) and (b) cover incidents involving critical
24	infrastructure assets or the activities of corporations to which
25	paragraph $51(xx)$ of the Constitution applies.
26	(5) However, subsection (4) does not make an entity liable to a civil
27	penalty under this Part if the incident:
28	(a) was not in fact effected by means of a telegraphic, telephonic
29	or other like service within the meaning of paragraph 51(v)
30	of the Constitution (including, for example, by means of the
31	internet); or
32	(b) did not in fact impede or impair the ability of a computer to
33	connect to such a service; or
34	(c) did not in fact seriously prejudice:
35	(i) the social or economic stability of Australia or its
36	people; or

1 2		<ul><li>(ii) the defence of Australia; or</li><li>(iii) national security.</li></ul>
		( )
3	27 Obliga	tion to report following a ransomware payment
4	(1)	The reporting business entity must give the designated
5		Commonwealth body a report (a ransomware payment report) that
6 7		complies with the requirements of this section within 72 hours of making the ransomware payment or becoming aware that the
8		ransomware payment has been made (whichever is applicable).
9		Note: For the definition of <i>designated Commonwealth body</i> : see section 8.
0	(2)	The ransomware payment report must contain information relating
1		to the following, in accordance with any requirements prescribed
12		by the rules, that, at the time of making the report, the reporting
13		business entity knows or is able, by reasonable search or enquiry,
14		to find out:
15		(a) if the reporting business entity made the payment—the
6		reporting business entity's contact and business details;
17 18		(b) if another entity made the payment—that entity's contact and business details;
9		(c) the cyber security incident, including its impact on the
20		reporting business entity;
21		(d) the demand made by the extorting entity;
22		(e) the ransomware payment;
23		(f) communications with the extorting entity relating to the
24		incident, the demand and the payment.
25	(3)	The reporting business entity may include other information
26		relating to the cyber security incident in the ransomware payment
27		report.
28	(4)	The ransomware payment report must be given:
29		(a) in the form approved by the Secretary (if any); and
30		(b) in the manner (if any) prescribed by the rules.
31	(5)	An entity is liable to a civil penalty if the entity contravenes
32		subsection (1).

1		Civil penalty: 60 penalty units.
2	(6)	Subsection 93(2) of the Regulatory Powers Act does not apply in relation to a contravention of subsection (1) of this section.
4	28 Liabili	ty
5	(1)	An entity is not liable to an action or other proceeding for damages
6		for or in relation to an act done or omitted in good faith in
7		compliance with section 27.
8	(2)	An officer, employee or agent of an entity is not liable to an action
9		for damages for or in relation to an act done or omitted in good
10		faith in connection with an act done or omitted by the entity as
11		mentioned in subsection (1).
12	(3)	An entity that wishes to rely on subsection (1) in relation to an
13		action or other proceeding bears an evidential burden (within the
14		meaning of the Regulatory Powers Act) in relation to that matter.

## **Division 3—Protection of information**

2		re payment reports may only be used or disclosed for
3	peri	mitted purposes
4	Pern	nitted use and disclosure
5	(1) A de	esignated Commonwealth body may make a record of, use or
6 7	a rep	lose information provided in a ransomware payment report by porting business entity, but only for the purposes of one or
8		e of the following:
9	(a)	assisting the reporting business entity, and other entities acting on behalf of the reporting business entity, to respond
11		to, mitigate or resolve the cyber security incident;
12 13	(b)	performing functions or exercising powers under this Part or Part 6 as it applies to this Part;
14	(c)	proceedings under, or arising out of, section 137.1 or 137.2
15		of the Criminal Code (false and misleading information and
16		documents) that relate to this Act;
17	(d)	proceedings for an offence against section 149.1 of the
18		Criminal Code (which deals with obstruction of
19		Commonwealth public officials) that relates to this Act;
20	(e)	the performance of the functions of a Commonwealth body
21		relating to responding to, mitigating or resolving a cyber
22		security incident;
23	(f)	the performance of the functions of a State body relating to
24		responding to, mitigating or resolving a cyber security
25		incident;
26	(g)	the performance of the functions of the National Cyber
27		Security Coordinator under Part 4 relating to a cyber security
28	4.	incident;
29	(h)	informing and advising the Minister, and other Ministers of
30	41)	the Commonwealth, about a cyber security incident;
31	(i)	the performance of the functions of an intelligence agency.
32	Note:	
33 34		of this Act unless a Minister of the State or Territory has consented to those Parts applying to the State body: see section 11.

1	Restriction on use and disclosure for civil or regulatory action
2	(2) However, the designated Commonwealth body must not make a
3	record of, use or disclose the information for the purposes of
4	investigating or enforcing, or assisting in the investigation or
5	enforcement of, any contravention by the reporting business entity
6	of a Commonwealth, State or Territory law other than:
7	(a) a contravention by the reporting business entity of this Part;
8	or
9	(b) a contravention by the reporting business entity of a law that
10	imposes a penalty or sanction for a criminal offence.
11 12	Note: See also section 32 in relation to admissibility of the information in proceedings against the reporting business entity.
13	Interaction with the Privacy Act 1988
14	(3) Subsection (1) does not authorise the designated Commonwealth
15	body to record, use or disclose the information to the extent that it
16	is prohibited or restricted by or under the Privacy Act 1988.
17	Information not covered by the prohibitions in this section
18	(4) Subsection (1) does not prohibit the recording, use or disclosure of
19	the following information:
20	(a) information that has been provided to the designated
21	Commonwealth body by, or on behalf of, the entity to the
22	Commonwealth to comply with:
23	(i) a requirement in Part 2B of the Security of Critical
24	Infrastructure Act 2018; or
25	(ii) a requirement under the Telecommunications Act 1997;
26	or
27	(iii) a requirement under a law prescribed by the rules;
28	(b) information that has already been lawfully made available to
29	the public.
30	30 Limitations on secondary use and disclosure of information in
31	ransomware payment reports
J 1	• • •
32	(1) This section applies to information that:

1 2	(a)	has been provided in a ransomware payment report by a reporting business entity; and
3 4	(b)	has been obtained by another entity, Commonwealth body or State body under subsection 29(1) or this section; and
5 6	(c)	is held by the other entity, Commonwealth body or State body.
7 8 9	Note:	This section does not apply to the information to the extent that it has been otherwise obtained by the other entity, Commonwealth body or State body.
10	Pern	uitted use and disclosure
11 12 13	recor	other entity, Commonwealth body or State body may make a rd of, use or disclose the information but only for the purposes see or more of the following:
14 15 16	(a)	assisting the reporting business entity, and other entities acting on behalf of the reporting business entity, to respond to, mitigate or resolve the cyber security incident;
17 18	(b)	performing functions or exercising powers under this Part or Part 6 as it applies to this Part;
19 20 21	(c)	proceedings under, or arising out of, section 137.1 or 137.2 of the <i>Criminal Code</i> (false and misleading information and documents) that relate to this Act;
22 23 24	(d)	proceedings for an offence against section 149.1 of the <i>Criminal Code</i> (which deals with obstruction of Commonwealth public officials) that relates to this Act;
25 26 27	(e)	the performance of the functions of a Commonwealth body relating to responding to, mitigating or resolving a cyber security incident;
28 29 30	(f)	the performance of the functions of a State body relating to responding to, mitigating or resolving a cyber security incident;
31 32 33	(g)	the performance of the functions of the National Cyber Security Coordinator under Part 4 relating to a cyber security incident;
34 35	(h)	informing and advising the Minister, and other Ministers of the Commonwealth, about a cyber security incident;
36	(i)	the performance of the functions of an intelligence agency.

1	Restriction on use and disclosure for civil or regulatory action
2 3	(3) However, the other entity, Commonwealth body or State body must not make a record of, use or disclose the information for the
4	purposes of investigating or enforcing, or assisting in the
5	investigation or enforcement of, any contravention, by the
6	reporting business entity, of a Commonwealth, State or Territory
7	law other than:
8	(a) a contravention by the reporting business entity of this Part;
9	or
10	(b) a contravention by the reporting business entity of a law that
11	imposes a penalty or sanction for a criminal offence.
12	Interaction with the Privacy Act 1988
13	(4) Subsection (2) does not authorise the other entity, Commonwealth
14	body or State body to record, use or disclose the information to the
15	extent that it is prohibited or restricted by or under the Privacy Act
16	1988.
17	Information not covered by the prohibitions in this section
18	(5) Subsection (2) does not prohibit:
19	(a) recording, use or disclosure of information referred to in
20	subsection 29(4); or
21	(b) if the other entity is an individual—recording, use or
22	disclosure of personal information about the individual; or
23	(c) recording, use or disclosure of the reporting business entity's
24	own information, with the consent of the reporting business
25	entity, by another entity, a Commonwealth body or a State
26	body; or
27	(d) recording, use or disclosure of information for the purposes
28	of carrying out a State's constitutional functions, powers or
29	duties.
30	Civil penalty for contravention of this section
31	(6) An entity is liable to a civil penalty if:
32	(a) the entity contravenes subsection (2); and
33	(b) the entity is not a Commonwealth officer; and

1	(c) any of the following applies:		
2	(i) the information is sensitive information about an		
3	individual and the individual has not consented to the		
4	record, use or disclosure of the information;		
5	(ii) the information is confidential or commercially		
6	sensitive;		
7	(iii) the record, use or disclosure of the information would,		
8	or could reasonably be expected to, cause damage to the		
9	security, defence or international relations of the		
10	Commonwealth.		
11	Note 1: See the <i>Criminal Code</i> for offences for Commonwealth officers.		
12 13	Note 2: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.		
14	Civil penalty: 60 penalty units.		
15	31 Legal professional privilege		
16	(1) The fact that a reporting business entity provided information in a		
17	ransomware payment report does not otherwise affect a claim of		
18	legal professional privilege that anyone may make in relation to		
19	that information in any proceedings:		
20	(a) under any Commonwealth, State or Territory law (including		
21	the common law); or		
22	(b) before a tribunal of the Commonwealth, a State or a		
23	Territory.		
24	(2) Despite subsection (1), this section does not apply to the following:		
25	(a) the proceedings of a coronial inquiry or a Royal Commission		
26	in Australia;		
27	(b) proceedings in a federal court exercising original jurisdiction		
28	in which a writ of mandamus or prohibition or an injunction		
29	is sought against an officer or officers of the Commonwealth.		
30	Note: For <i>federal court</i> , see section 2B of the <i>Acts Interpretation Act</i>		
31	1901.		
32	(3) This section does not limit or affect any right, privilege or		
33	immunity that the reporting business entity has, apart from this		
34	section, as a defendant in any proceedings.		

2	against reporting business entity
3	(1) This section applies to information that:
4	(a) has been provided in a ransomware payment report by a
5	reporting business entity; and
6	(b) has been obtained by a Commonwealth body or State body
7	under section 27, subsection 29(1) or section 30; and
8	(c) is held by the Commonwealth body or State body.
9	Note: This section does not apply to information held by the Commonwealt body or State body to the extent that it has been otherwise obtained.
1	(2) That information is not admissible in evidence against the
2	reporting business entity in any of the following proceedings:
13	(a) criminal proceedings for an offence against a
4	Commonwealth, State or Territory law, other than:
15	(i) proceedings for an offence against section 137.1 or
6	137.2 of the <i>Criminal Code</i> (which deal with false or
17	misleading information or documents) that relates to
8	this Act; or
9	(ii) proceedings for an offence against section 149.1 of the
20	Criminal Code (which deals with obstruction of
21	Commonwealth public officials) that relates to this Act;
22	(b) civil proceedings for a contravention of a civil penalty
23	provision of a Commonwealth, State or Territory law, other
24	than a civil penalty provision of this Part;
25	(c) proceedings for a breach of any other Commonwealth, State
26	or Territory law (including the common law);
27	(d) proceedings before a tribunal of the Commonwealth, a State
28	or a Territory.
29	(3) However, this section does not apply to the following:
80	(a) the proceedings of a coronial inquiry or a Royal Commission
31	in Australia;
32	(b) proceedings in a federal court exercising original jurisdiction
33	in which a writ of mandamus or prohibition or an injunction
34	is sought against an officer or officers of the Commonwealth

# Part 3 Ransomware reporting obligationsDivision 3 Protection of information

1 2	Note: For federal court, see section 2B of the <i>Acts Interpretation Act</i> 1901.
3	(4) This section does not limit or affect any right, privilege or
4	immunity that the reporting business entity has, apart from this
5	section, as a defendant in any proceedings.

# Part 4—Coordination of significant cyber security incidents

### **Division 1—Preliminary**

2

3

4

13

14

15

16

17

18

19

20

21

22

23

#### 33 Simplified outline of this Part

Information may be voluntarily provided to the National Cyber Security Coordinator in relation to significant cyber security incidents.

The National Cyber Security Coordinator's role is to lead across the whole of Government the coordination and triaging of action in response to a significant cyber security incident.

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

### 34 Meaning of significant cyber security incident

A cyber security incident is a *significant cyber security incident* if:

- (a) there is a material risk that the incident has seriously prejudiced, is seriously prejudicing, or could reasonably be expected to prejudice:
  - (i) the social or economic stability of Australia or its people; or
  - (ii) the defence of Australia; or
- (iii) national security; or
- (b) the incident is, or could reasonably be expected to be, of serious concern to the Australian people.

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

2	National Cyber Security Coordinator
3	35 Impacted entity may voluntarily provide information to National
4	Cyber Security Coordinator in relation to a significant
5	cyber security incident
6	(1) This section applies if:
7	(a) an incident has occurred, is occurring or is imminent; and
8	(b) the incident is a cyber security incident; and
9	(c) the incident has had, is having, or could reasonably be
10	expected to have, a direct or indirect impact on an entity (the
11	impacted entity); and
12	(d) the impacted entity is:
13	(i) carrying on a business in Australia; or
14	(ii) a responsible entity for a critical infrastructure asset to
15	which the Security of Critical Infrastructure Act 2018
16	applies.
17	(2) The impacted entity, or another entity acting on behalf of the
18	impacted entity, may provide information about the incident to the
19	National Cyber Security Coordinator if:
20	(a) the incident is a significant cyber security incident; or
21	(b) the incident could reasonably be expected to be a significant
22	cyber security incident.
23	Note 1: For information provided in relation to other kinds of cyber security
24	incidents: see sections 36 and 39.
25	Note 2: This subsection constitutes an authorisation for the National Cyber
26 27	Security Coordinator to collect the information (including sensitive information) for the purposes of the <i>Privacy Act 1988</i> .
<i>21</i>	information) for the purposes of the 1 tivacy Act 1700.
28	(3) Information about the incident may be provided under
29	subsection (2):
30	(a) at any time during the response to the incident; and
31	(b) on the impacted entity's own initiative or in response to a
32	request by the National Cyber Security Coordinator.

Presumption  4 (4) For the purposes of paragraph (1)(b), an incident covered by paragraph 9(2)(a) or (b) cyber security incident if:  7 (a) the incident was probably effected, is paragraph or could reasonably be expected to be telegraphic, telephonic or other like seem meaning of paragraph 51(v) of the Conformation of the internet):  (b) the initial telephonic and the internet):	or is presumed to be a probably being effected effected, by means of a rvice within the astitution (including, or mpaired, or is probably
incident covered by paragraph 9(2)(a) or (b) cyber security incident if:  (a) the incident was probably effected, is por could reasonably be expected to be telegraphic, telephonic or other like semeaning of paragraph 51(v) of the Corfor example, by means of the internet):	or is presumed to be a probably being effected effected, by means of a rvice within the astitution (including, or mpaired, or is probably
cyber security incident if:  (a) the incident was probably effected, is part or could reasonably be expected to be telegraphic, telephonic or other like seem meaning of paragraph 51(v) of the Corfor example, by means of the internet):	probably being effected effected, by means of a rvice within the astitution (including, ; or mpaired, or is probably
7 (a) the incident was probably effected, is p 8 or could reasonably be expected to be 9 telegraphic, telephonic or other like ser 10 meaning of paragraph 51(v) of the Cor 11 for example, by means of the internet):	effected, by means of a rvice within the astitution (including, or mpaired, or is probably
or could reasonably be expected to be telegraphic, telephonic or other like set meaning of paragraph 51(v) of the Cor for example, by means of the internet):	effected, by means of a rvice within the astitution (including, or mpaired, or is probably
telegraphic, telephonic or other like set meaning of paragraph 51(v) of the Cor for example, by means of the internet):	rvice within the astitution (including, ; or mpaired, or is probably
meaning of paragraph 51(v) of the Cor for example, by means of the internet):	nstitution (including, ; or mpaired, or is probably
for example, by means of the internet):	; or mpaired, or is probably
* * *	mpaired, or is probably
(b) the incident has probably impeded or i	
impeding or impairing or could reason impede or impair, the ability of a comp	
• • • • • • • • • • • • • • • • • • • •	buter to connect to such
•	indicad is probably
16 (c) the incident has probably seriously pre- 17 seriously prejudicing, or could reasona	
18 prejudice:	by be expected to
(i) the social or economic stability of	f Australia or its
20 people; or	1 / tustrana or its
21 (ii) the defence of Australia; or	
(iii) national security.	
Note: Paragraphs 9(2)(a) and (b) covers incident	a involving oritical
24 infrastructure assets or the activities of cor	
paragraph 51(xx) of the Constitution appli	
(5) However, subsection (4) does not make an e	ntity liable to a civil
penalty under this Part if the incident:	
28 (a) was not in fact effected by means of a	
or other like service within the meanin	
of the Constitution (including, for example)	mple, by means of the
internet); or	
32 (b) did not in fact impede or impair the ab	ility of a computer to
connect to such a service; or	
(c) did not in fact seriously prejudice:	
(i) the social or economic stability of	f Australia or its
people; or	

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

$\alpha$	. •	20
· ·	ection	3h
v	CCHOIL	20

1	(ii) the defence of Australia; or
2	(iii) national security.
3	36 Voluntary provision of information in relation to other incidents
4	or cyber security incidents
5	(1) This section applies if:
6	(a) an incident has occurred, is occurring or is imminent; and
7 8 9	<ul> <li>(b) an entity (the <i>impacted entity</i>) provides information to the National Cyber Security Coordinator in relation to the incident; and</li> </ul>
10	(c) it is unclear at the time the information is provided whether the incident is a cyber security incident or a significant cyber
12	security incident.
13 14	(2) The National Cyber Security Coordinator may collect and use the information for the purposes of determining whether the incident is a cyber security incident or a significant cyber security incident.
16 17 18	Note: This subsection constitutes an authorisation for the National Cyber Security Coordinator to collect the information (including sensitive information) for the purposes of the <i>Privacy Act 1988</i> .
19	37 Role of the National Cyber Security Coordinator
20	The role of the National Cyber Security Coordinator includes, but
21	is not limited to, the following:
22	(a) to lead across the whole of Government the coordination and
23 24	triaging of action in response to a significant cyber security incident;
25	(b) to inform and advise the Minister and the whole of
26 27	Government in relation to the whole of Government response to a significant cyber security incident.

### **Division 3—Protection of information**

2		n provided in relation to a significant cyber security
3		ident—use and disclosure by National Cyber Security
4	Co	ordinator
5	Per	mitted use and disclosure
6	(1) The	National Cyber Security Coordinator may make a record of,
7		or disclose information provided under subsection 35(2) by, or
8		behalf of, an entity (the <i>impacted entity</i> ) in relation to a cyber
9 10		urity incident but only for the purposes of one or more of the owing:
11		) assisting the impacted entity, and other entities acting on
12		behalf of the impacted entity, to respond to, mitigate or
13		resolve the cyber security incident;
14	(b	) a permitted cyber security purpose for a cyber security
15	<b>(</b> -	incident.
16	Note	e 1: For <i>permitted cyber security purpose</i> for a cyber security incident: se
17 18		section 10. This includes the functions of the National Cyber Security Coordinator under this Part.
19	Note	2: Certain information must not be disclosed to a State body under Parts
20 21		of this Act unless a Minister of the State or Territory has consented to those Parts applying to the State body: see section 11.
22	Res	triction on use and disclosure for civil or regulatory action
23	(2) Hov	wever, the National Cyber Security Coordinator must not make
24	a re	cord of, use or disclose the information for the purposes of
25		estigating or enforcing, or assisting in the investigation or
26		orcement of, any contravention by the impacted entity of a
27	Cor	nmonwealth, State or Territory law other than:
28	(a	) a contravention by the impacted entity of this Part; or
29	(b	) a contravention by the impacted entity of a law that imposes
30		a penalty or sanction for a criminal offence.
31	Note	See also section 42 in relation to admissibility of the information in
32		proceedings against the impacted entity.

1	Interaction with the Privacy Act 1988
2	(3) Subsection (1) does not authorise the National Cyber Security
3	Coordinator to record, use or disclose the information to the extent
4	that it is prohibited or restricted by or under the <i>Privacy Act 1988</i> .
5	Information not covered by the prohibitions in this section
6	(4) Subsection (1) does not prohibit the recording, use or disclosure of
7	the following information:
8	(a) information that has been provided by, or on behalf of, the
9	impacted entity to the Commonwealth about the cyber
10	security incident to comply with:
11	(i) a requirement in Part 3 of this Act; or
12	(ii) a requirement in Part 2B of the Security of Critical
13	Infrastructure Act 2018; or
14	(iii) a requirement under the Telecommunications Act 1997;
15	or
16	(iv) a requirement under a law prescribed by the rules;
17	(b) information that has been provided voluntarily to the
18	National Cyber Security Coordinator by, or on behalf of, the
19	impacted entity, other than under this Part;
20	(c) information that has already been lawfully made available to
21	the public.
22	39 Information provided in relation to other incidents—use and
23	disclosure by National Cyber Security Coordinator
24	(1) This section applies if:
25	(a) an incident has occurred, is occurring or is imminent; and
26	(b) an entity (the <i>impacted entity</i> ) provides information to the
27	National Cyber Security Coordinator in relation to the
28	incident; and
29	(c) the incident either:
30	(i) is not a cyber security incident; or
31	(ii) is a cyber security incident but is not a significant cyber
32	security incident.

1	Permitted use and disclosure
2	(2) The National Cyber Security Coordinator may make a record of,
3	use or disclose the information provided by the impacted entity but
4	only for the purposes of one or more of the following:
5	(a) directing the impacted entity to other services that may assist
6	the entity to respond to, mitigate, or resolve the incident;
7	(b) if the incident is a cyber security incident—coordinating the
8	whole of Government response to the cyber security incident
9	where the National Cyber Security Coordinator considers
10	such a response is necessary;
11	(c) if the incident is a cyber security incident—informing and
12	advising the Minister, and other Ministers of the
13	Commonwealth, about the cyber security incident.
14	Restriction on use and disclosure for civil or regulatory action
15	(3) However, the National Cyber Security Coordinator must not make
16	a record of, use or disclose the information for the purposes of
17	investigating or enforcing, or assisting in the investigation or
18	enforcement of, any contravention by the impacted entity of a
19	Commonwealth, State or Territory law other than:
20	(a) a contravention by the impacted entity of this Part; or
21 22	(b) a contravention by the impacted entity of a law that imposes a penalty or sanction for a criminal offence.
23	Note: See also section 42 in relation to admissibility of the information in
24	proceedings against the impacted entity.
25	Interaction with the Privacy Act 1988
26	(4) Subsection (2) does not authorise the National Cyber Security
27	Coordinator to record, use or disclose the information to the extent
28	that it is prohibited or restricted by or under the <i>Privacy Act 1988</i> .
29	Information not covered by the prohibitions in this section
30	(5) Subsection (2) does not prohibit the recording, use or disclosure of
31	the following information:
	-

1 2		nformation that has been provided by, or on behalf of, the mpacted entity to the Commonwealth about the cyber
3	S	ecurity incident to comply with:
4		(i) a requirement in Part 3 of this Act; or
5 6		(ii) a requirement in Part 2B of the Security of Critical Infrastructure Act 2018; or
7	(	iii) a requirement under the <i>Telecommunications Act 1997</i> ;
8	`	or
9	(	(iv) a requirement under a law prescribed by the rules;
10	(b) i	nformation that has been provided voluntarily to the
11 12		National Cyber Security Coordinator by, or on behalf of, the mpacted entity, other than under this Part;
13	(c) i	nformation that has already been lawfully made available to
14	t]	he public.
15	40 Limitations o	n secondary use and disclosure
16	(1) This se	ection applies to information that:
17	(a) h	has been provided by, or on behalf of, an entity (the impacted
18 19		<i>entity</i> ) under subsection 35(2) or as referred to in ubsection 39(1); and
20	(b) h	has been obtained by another entity, a Commonwealth body
21 22		other than ASD) or a State body under subsection 38(1) or 39(2) or this section; and
23	(c) is	s held by the other entity, Commonwealth body or State
24	· ·	oody.
25	Note 1:	This section does not apply to the information to the extent that it has
26 27		been otherwise obtained by the other entity, Commonwealth body or State body.
	N . 0	,
28 29	Note 2:	For ASD, see Division 1A of Part 6 of the <i>Intelligence Services Act</i> 2001.
30	Permit	ted use and disclosure
21	(2) The of	her entity, Commonwealth body or State body may make a
31 32		of, use or disclose the information but only for the purposes
33		or more of the following:

1 2	(a) assisting the impacted entity, and other entities acting on behalf of the impacted entity, to respond to, mitigate or
3	resolve the cyber security incident;
4 5	<ul><li>(b) a permitted cyber security purpose for a cyber security incident.</li></ul>
6 7	Note: For <i>permitted cyber security purpose</i> for a cyber security incident: see section 10.
8	Restriction on use and disclosure for civil or regulatory action
9	(3) However, the other entity, Commonwealth body or State body
10	must not make a record of, use or disclose the information for the
11	purposes of investigating or enforcing, or assisting in the
12	investigation or enforcement of, any contravention by the impacted
13	entity of a Commonwealth, State or Territory law other than:
14	(a) a contravention by the impacted entity of this Part; or
15	(b) a contravention by the impacted entity of a law that imposes
16	a penalty or sanction for a criminal offence.
17	Interaction with the Privacy Act 1988
18	(4) Subsection (2) does not authorise the other entity, Commonwealth
19	body or State body to record, use or disclose the information to the
20	extent that it is prohibited or restricted by or under the <i>Privacy Act</i>
21	1988.
22	Information not covered by the prohibitions in this section
23	(5) Subsection (2) does not prohibit:
24	(a) recording, use or disclosure of information referred to in
25	subsection 38(4) or 39(5); or
26	(b) if the other entity is an individual—recording, use or
27	disclosure of personal information about the individual; or
28	(c) recording, use or disclosure of the impacted entity's own
29	information, with the consent of the impacted entity, by
30	another entity, a Commonwealth body or a State body; or
31	(d) recording, use or disclosure for the purposes of carrying out a
32	State's constitutional functions, powers or duties.

1	Civil penalty for contravention of this section
2	(6) An entity is liable to a civil penalty if:
3	(a) the entity contravenes subsection (2); and
4	(b) the entity is not a Commonwealth officer; and
5	(c) any of the following applies:
6	(i) the information is sensitive information about an
7	individual and the individual has not consented to the
8	record, use or disclosure of the information;
9 10	<ul><li>(ii) the information is confidential or commercially sensitive;</li></ul>
11	(iii) the record, use or disclosure of the information would,
12	or could reasonably be expected to, cause damage to the
13	security, defence or international relations of the
14	Commonwealth.
15	Note 1: See the <i>Criminal Code</i> for offences for Commonwealth officers.
16 17	Note 2: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.
18	Civil penalty: 60 penalty units.
19	41 Legal professional privilege
20	(1) The fact that an entity provided information to the National Cyber
21	Security Coordinator under subsection 35(2), or as referred to in
22	subsection 39(1), does not otherwise affect a claim of legal
23	professional privilege that anyone may make in relation to that
24	information in any proceedings:
25	(a) under any Commonwealth, State or Territory law (including
26	the common law); or
27	(b) before a tribunal of the Commonwealth, a State or a
28	Territory.
29	(2) Despite subsection (1), this section does not apply to the following:
30	(a) the proceedings of a coronial inquiry or a Royal Commission
31	in Australia;

1 2	(b) proceedings in a federal court exercising original jurisdiction in which a writ of mandamus or prohibition or an injunction
3	is sought against an officer or officers of the Commonwealth.
4 5	Note: For <i>federal court</i> , see section 2B of the <i>Acts Interpretation Act</i> 1901.
6	(3) This section does not limit or affect any right, privilege or
7	immunity that the entity has, apart from this section, as a defendant
8	in any proceedings.
9	42 Admissibility of information voluntarily given by impacted entity
10	(1) This section applies to information that:
11	(a) has been provided by, or on behalf of, an entity (the impacted
12	entity) under subsection 35(2) or as referred to in
13	subsection 39(1); and
14	(b) has been obtained by a Commonwealth body or State body
15	under subsection 35(2), 38(1), 39(1), 39(2) or 40(2); and
16	(c) is held by the Commonwealth body or State body.
17 18	Note: This section does not apply to information held by the Commonwealth body or State body to the extent that it has been otherwise obtained.
19	(2) That information is not admissible in evidence against the
20	impacted entity in any of the following proceedings:
21	(a) criminal proceedings for an offence against a
22	Commonwealth, State or Territory law, other than:
23	(i) proceedings for an offence against section 137.1 or
24	137.2 of the <i>Criminal Code</i> (which deal with false or
25	misleading information or documents) that relates to
26	this Act; or
27	(ii) proceedings for an offence against section 149.1 of the
28	Criminal Code (which deals with obstruction of
29	Commonwealth public officials) that relates to this Act;
30	(b) civil proceedings for a contravention of a civil penalty
31	provision of a Commonwealth, State or Territory law, other
32	than a civil penalty provision of this Part;
33	(c) proceedings for a breach of any other Commonwealth, State
34	or Territory law (including the common law);

1 2	(d) proceedings before a tribunal of the Commonwealth, a State or a Territory.
3	(3) However, this section does not apply to the following:
4	(a) the proceedings of a coronial inquiry or a Royal Commission
5	in Australia;
6	(b) proceedings in a federal court exercising original jurisdiction
7	in which a writ of mandamus or prohibition or an injunction
8	is sought against an officer or officers of the Commonwealth.
9 10	Note: For <i>federal court</i> , see section 2B of the <i>Acts Interpretation Act</i> 1901.
11	(4) This section does not limit or affect any right, privilege or
12	immunity that the entity has, apart from this section, as a defendant
13	in any proceedings.
14	43 National Cyber Security Coordinator not compellable as witness
15	(1) The Secretary may issue a certificate stating that:
16	(a) a specified person is, or has been:
17	(i) a person referred to in paragraph (a) of the definition of
18	National Cyber Security Coordinator in section 8; or
19	(ii) a person referred to in paragraph (b) of the definition of
20	National Cyber Security Coordinator in section 8; and
21	(b) the specified person is involved, or has been involved, in a
22	specified matter in which the National Cyber Security
23	Coordinator is performing or has performed functions or is
24	exercising or has exercised powers under this Part.
25	(2) If, under subsection (1), the Secretary issues a certificate in relation
26	to a person and a specified matter, the person:
27	(a) is not obliged to comply with a subpoena or similar direction
28	of a federal court or a court of a State or Territory to attend
29	and answer questions relating to the matter; and
30	(b) is not compellable to give an expert opinion in any civil or
31	criminal proceedings in a federal court or a court of a State or
32	Territory in relation to the matter:

No. , 2024

# Coordination of significant cyber security incidents **Part 4**Protection of information **Division 3**

### Section 43

1	but only to the extent that the matter relates to information that has
2	been provided by, or on behalf of, an entity under subsection 35(2)
3	or as referred to in subsection 39(1).

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

## **Division 4—Miscellaneous**

2		th other requirements to provide information in
3	relatio	n to a cyber security incident
4	Informa	ation provided by an entity under this Part does not affect
5	any oth	er requirement of the entity to provide that information
6	under th	his Act or another law of the Commonwealth.
7	Note:	For example, the entity may also be required to provide some or all of
8		the information under Part 3 of this Act, Part 2B of the Security of
9		Critical Infrastructure Act 2018 or under the Telecommunications Act
10		1997.

# Part 5—Cyber Incident Review Board

### Division 1—Preliminary

2

3

#### 45 Simplified outline of this Part

The Cyber Incident Review Board is established by this Part. 4 The Board must cause reviews to be conducted in relation to 5 certain cyber security incidents. The purpose of a review is to make 6 recommendations to government and industry about actions that 7 could be taken to prevent, detect, respond to or minimise the 8 impact of, cyber security incidents of a similar nature in the future. 9 A review panel will be established for each review in accordance 10 with the terms of reference for the review. 11 The Board consists of the Chair and up to 6 other standing 12 members. The standing members are appointed by the Minister. 13 The Board may establish an Expert Panel. One or more members 14 of the Expert Panel may be appointed to assist in relation to a 15 review conducted under this Part. 16 This Part also deals with the appointment of the Chair, standing 17 members and Expert Panel members, and the procedures of the 18 Board. 19

### **Division 2—Reviews**

46 Board n	nust cause reviews to be conducted
į	The Cyber Incident Review Board may cause a review to be conducted under this section in relation to a cyber security incident, or a series of related cyber security incidents, on written referral by:
	(a) the Minister; or
	(b) the National Cyber Security Coordinator; or
	(c) an entity impacted by the incident or an incident in the series of incidents; or
	(d) a member of the Board.
1	Note: Each review is conducted by a particular review panel established for that review in accordance with the terms of reference for the review.
(2)	A review may only be conducted under this section:
	(a) if the Board is satisfied that the incident or series of incidents meets the criteria mentioned in subsection (3); and
	(b) after the incident or series of incidents, and the immediate response, has ended; and
	(c) if the Minister has approved the terms of reference for the review.
(3)	For the purposes of paragraph (2)(a), the criteria are:
	<ul><li>(a) the incident or series of incidents have seriously prejudiced, or could reasonably be expected to seriously prejudice:</li><li>(i) the social or economic stability of Australia or its</li></ul>
	people; or
	(ii) the defence of Australia; or
	(iii) national security; or
	(b) the incident or series of incidents involved novel or complex methods or technologies, an understanding of which will significantly improve Australia's preparedness, resilience, or response to cyber security incidents of a similar nature; or
	(c) the incident or series of incidents are, or could reasonably be

expected to be, of serious concern to the Australian people.

No. , 2024

2 (a) the Chair; and	
<ul> <li>(b) the standing members of the Board that are spec</li> <li>terms of reference for the review; and</li> </ul>	rified in the
5 (c) the members of the Expert Panel appointed to as	ssist in the
review under section 70.	
7 The terms of reference for the review must specify one	e or more
standing members for the review.	
9 (5) The rules may make provision for or in relation to revi	iews under
this Part, including for or in relation to the following:	
(a) dealing with written referrals made to the Board	ļ <b>;</b>
(b) prioritisation of referrals for review and reviews	conducted;
(c) terms of reference for reviews, including their va	ariation;
(d) notification of reviews;	
(e) the timing of when reviews may be conducted;	
(f) when reviews may be discontinued;	
(g) how information or submissions may be provide	ed for
reviews.	
47 Board may discontinue a review	
(1) The Board may discontinue a review at any time.	
(2) The Board must, within 28 days of discontinuing a rev	view, publish
in any way the Board considers appropriate notice of t	
being discontinued.	
48 Chair may request information or documents	
25 If the Board reasonably believes that:	
26 (a) an entity; or	
(b) a Commonwealth body or a State body; or	
(c) an officer or employee of a Commonwealth bod	ly or a State
body;	-
has information or documents relevant to a review bei	ing conducted
under section 46 by a review panel, the Chair may req	•
notice in writing, the entity, body, officer or employee	e to give the

1 2	Board such information or documents as are specified in the request.
3	Note 1: There is no requirement to comply with the request.
4 5	Note 2: The Chair may require certain entities to give documents under section 49.
6	49 Chair may require certain entities to produce documents
7	(1) This section applies if:
8	(a) the Board reasonably believes that an entity involved in a
9	cyber security incident that relates to a review being
10 11	conducted under section 46 by a review panel has a document that is relevant to the review; and
12	(b) the Chair of the Board has requested that the entity provide
13	the document under section 48; and
14	(c) the entity is not:
15	(i) a Commonwealth body or a State body; or
16	(ii) an officer or employee of a Commonwealth body or a
17	State body.
18	(2) The Chair of the Board may, by notice in writing given to the
19	entity, require the entity to:
20	(a) produce any such documents; or
21	(b) make copies of any such documents and to produce those
22	copies;
23	to the Board within the period (which must not be less than 14
24	days), and in the manner, specified in the notice.
25	(3) The notice must set out the effect of the following provisions:
26	(a) section 50;
27	(b) Part 6 of this Act (Regulatory powers);
28	(c) sections 137.1 and 137.2 of the Criminal Code (false or
29	misleading information or documents).

1	Compensation
2	(4) An entity is entitled to be paid by the Commonwealth reasonable compensation for complying with a requirement covered by
4	paragraph (2)(b).
5	50 Civil penalty—failing to comply with a notice to produce
6	documents
7	(1) An entity is liable to a civil penalty if:
8	(a) the entity is given a notice under subsection 49(2); and
9	(b) the entity fails to comply with the notice.
10	Civil penalty: 60 penalty units.
11	(2) Subsection (1) does not apply in relation to the production of a
12	document or a copy of a document if the production would, or
13	could reasonably be expected to, prejudice one or more of the
14	following:
15 16	(a) the security, defence or international relations of the Commonwealth;
17	(b) the capabilities of an intelligence agency;
18	(c) the prevention, detection or investigation of, or the conduct
19	of proceedings relating to, an offence or a contravention of a
20	civil penalty provision;
21	(d) the administration of justice.
22	(3) Subsection 93(2) of the Regulatory Powers Act does not apply in
23	relation to a contravention of subsection (1) of this section.
24	(4) Despite section 96 of the Regulatory Powers Act, in proceedings
25	for a civil penalty order against an entity for a contravention of
26	subsection (1), the entity does not bear an evidential burden in
27	relation to the matters in subsection (2).
28 29	Note: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.

51	Draft	review	reports
----	-------	--------	---------

(1) The Board must prepare a draft report (a draft review report) on a review being conducted under section 46 by a review panel.  (2) The draft review report must set out: (a) the preliminary findings of the review; and (b) a summary of the information and material on which those preliminary findings are based; and (c) any recommendations the Board proposes to make; and (d) if the Board proposes to make recommendations—the reasons for those proposed recommendations; and (e) if the terms of reference for the review require particular information to be included in the draft review report—that information; and (f) information (if any) that is prescribed by the rules; and (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board must give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity: (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or (b) for the purposes of determining whether information proposed to be included in the final review report is sensitiv review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity under subsection (4), the Board must specify a reasonable period		
(a) the preliminary findings of the review; and (b) a summary of the information and material on which those preliminary findings are based; and (c) any recommendations the Board proposes to make; and (d) if the Board proposes to make recommendations—the reasons for those proposed recommendations; and (e) if the terms of reference for the review require particular information to be included in the draft review report—that information; and (f) information (if any) that is prescribed by the rules; and (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or (b) for the purposes of determining whether information proposed to be included in the final review report is sensitiv review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		(1) The Board must prepare a draft report (a <i>draft review report</i> ) on a review being conducted under section 46 by a review panel.
(b) a summary of the information and material on which those preliminary findings are based; and  (c) any recommendations the Board proposes to make; and  (d) if the Board proposes to make recommendations—the reasons for those proposed recommendations; and  (e) if the terms of reference for the review require particular information to be included in the draft review report—that information; and  (f) information (if any) that is prescribed by the rules; and  (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	4	(2) The draft review report must set out:
preliminary findings are based; and  (c) any recommendations the Board proposes to make; and  (d) if the Board proposes to make recommendations—the reasons for those proposed recommendations; and  (e) if the terms of reference for the review require particular information to be included in the draft review report—that information; and  (f) information (if any) that is prescribed by the rules; and  (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitiv review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.	5	(a) the preliminary findings of the review; and
(c) any recommendations the Board proposes to make; and (d) if the Board proposes to make recommendations—the reasons for those proposed recommendations; and (e) if the terms of reference for the review require particular information to be included in the draft review report—that information; and (f) information (if any) that is prescribed by the rules; and (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or (b) for the purposes of determining whether information proposed to be included in the final review report is sensitiv review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		
(d) if the Board proposes to make recommendations—the reasons for those proposed recommendations; and  (e) if the terms of reference for the review require particular information to be included in the draft review report—that information; and  (f) information (if any) that is prescribed by the rules; and  (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	·	
reasons for those proposed recommendations; and  (e) if the terms of reference for the review require particular information to be included in the draft review report—that information; and  (f) information (if any) that is prescribed by the rules; and  (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		* *
information to be included in the draft review report—that information; and  (f) information (if any) that is prescribed by the rules; and  (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		* *
information to be included in the draft review report—that information; and  (f) information (if any) that is prescribed by the rules; and  (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	11	(e) if the terms of reference for the review require particular
(f) information (if any) that is prescribed by the rules; and (g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitiv review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		information to be included in the draft review report—that
(g) such other information that the Board thinks fit to include in the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		·
the draft review report.  (3) The Board must give the draft review report to the Minister.  (4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		
(4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		
draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	17	(3) The Board must give the draft review report to the Minister.
draft review report, to any other Commonwealth body or a State body or entity:  (a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	18	(4) The Board may give the draft review report, or an extract of the
(a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	19	
entity an opportunity to make submissions on the draft review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	20	body or entity:
review report or the extract; or  (b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	21	(a) if the Board considers it appropriate to give the body or
(b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		
proposed to be included in the final review report is sensitive review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		•
review information.  Note 1: The disclosure of sensitive review information may be prohibited under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		
under another Act (for example, the <i>Privacy Act 1988</i> ). This section does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		
does not authorise disclosure if prohibited under that Act: see subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	27	Note 1: The disclosure of sensitive review information may be prohibited
subsection (7) of this section.  Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	28	
Note 2: Sensitive review information must be redacted from a final review report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity		
report that is to be published by the Board: see section 53.  (5) If the Board gives a draft review report to the Minister under subsection (3), or a Commonwealth body, State body or entity	30	• •
subsection (3), or a Commonwealth body, State body or entity		
	33	
under subsection (4), the Board must specify a reasonable period	34	
	35	under subsection (4), the Board must specify a reasonable period

1 2	within which submissions may be made to the Board on the draft review report.
3 4	(6) Submissions must be given in the manner and form (if any) prescribed by the rules.
5 6 7	(7) However, this section does not authorise the Board to record, use or disclose the information to the extent that it is prohibited or restricted by or under the <i>Privacy Act 1988</i> or any other Act.
8 <b>52 Fin</b>	al review reports
9 10 11	(1) After a review is completed under section 46 by the review panel, the Board must prepare a report (a <i>final review report</i> ) on the review.
12 13	Note 1: The Board must redact sensitive review information from a final review report: see section 53.
14 15	Note 2: If information is redacted from a final review report, the Board must also prepare a protected review report: see section 54.
16 17 18	(2) In preparing the final review report, the Board must consider any submissions received under section 51 in relation to the draft review report.
19 20 21 22 23 24 25 26 27 28 29 30 31	<ul> <li>(3) Subject to section 53, the final review report must set out: <ul> <li>(a) the findings of the review; and</li> <li>(b) a summary of the information and material on which those findings are based; and</li> <li>(c) any recommendations made by the Board; and</li> <li>(d) if recommendations are made—the reasons for those recommendations; and</li> <li>(e) if the terms of reference for the review require particular information to be included in the review report—that information; and</li> <li>(f) information (if any) that is prescribed by the rules; and</li> <li>(g) such other information that the Board thinks fit to include in the report.</li> </ul> </li> </ul>
32	(4) The Board must not in the final review report:

1	(a) apportion blame in relation to a cyber security incident that was the subject of the review; or
2	
3	(b) provide the means to determine the liability of any entity in relation to such a cyber security incident; or
-	(c) identify an individual (unless the individual has consented);
5 6	or
7	(d) allow any adverse inference to be drawn from the fact that an
8	entity is the subject of the review.
9	However, even though blame or liability may be inferred, or an
0	adverse inference may be made, by a person other than the Board,
1	this does not prevent the Board from including information in the
12	final review report.
13	(5) This section does not otherwise limit what may be included in the
4	final review report.
15	(6) The Board must publish the final review report (excluding any
6	information required to be redacted under section 53). The report
17	may be published in any way the Board considers appropriate.
18	53 Certain information must be redacted from final review reports
	•
19	<ul><li>53 Certain information must be redacted from final review reports</li><li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review</li></ul>
19 20	(1) Information must be redacted from a final review report if the
19 20 21	(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.
19 20 21	(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.  Note: If information is redacted from a final review report, the Board must
19 20 21 22 23	(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.
18 20 21 22 23 24	<ul> <li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.</li> <li>Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.</li> <li>(2) Sensitive review information is information the disclosure of</li> </ul>
20 21 22 23 24	(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.  Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.
20 21 22 23 24	<ul> <li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.</li> <li>Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.</li> <li>(2) Sensitive review information is information the disclosure of</li> </ul>
20 21 22 23 24 25	<ul> <li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.</li> <li>Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.</li> <li>(2) Sensitive review information is information the disclosure of which:</li> </ul>
20 21 22 23 24 25 26	<ol> <li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.</li> <li>Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.</li> <li>(2) Sensitive review information is information the disclosure of which:         <ul> <li>(a) could prejudice the security, defence or international relations of Australia; or</li> <li>(b) would prejudice relations between the Commonwealth</li> </ul> </li> </ol>
19 20 21 22 23 24 25 26 27	<ul> <li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.</li> <li>Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.</li> <li>(2) Sensitive review information is information the disclosure of which: <ul> <li>(a) could prejudice the security, defence or international relations of Australia; or</li> </ul> </li> </ul>
20 21 22 23 24 25 26 27 28	<ol> <li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.</li> <li>Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.</li> <li>(2) Sensitive review information is information the disclosure of which:         <ul> <li>(a) could prejudice the security, defence or international relations of Australia; or</li> <li>(b) would prejudice relations between the Commonwealth government and the government of a State or Territory; or</li> <li>(c) could reveal, or enable a person to ascertain, the existence or</li> </ul> </li> </ol>
20 21 22 23 24 25 26 27 28 29	<ol> <li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.</li> <li>Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.</li> <li>(2) Sensitive review information is information the disclosure of which:         <ul> <li>(a) could prejudice the security, defence or international relations of Australia; or</li> <li>(b) would prejudice relations between the Commonwealth government and the government of a State or Territory; or</li> <li>(c) could reveal, or enable a person to ascertain, the existence or identity of a confidential source of information in relation to</li> </ul> </li> </ol>
99 200 211 222 233 244 255 266 277 288 899 99	<ol> <li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.</li> <li>Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.</li> <li>(2) Sensitive review information is information the disclosure of which:         <ul> <li>(a) could prejudice the security, defence or international relations of Australia; or</li> <li>(b) would prejudice relations between the Commonwealth government and the government of a State or Territory; or</li> <li>(c) could reveal, or enable a person to ascertain, the existence or</li> </ul> </li> </ol>
99 200 21 222 233 244 255 266 277 288 299 300 311 322	<ol> <li>(1) Information must be redacted from a final review report if the Chair is satisfied that the information is sensitive review information.</li> <li>Note: If information is redacted from a final review report, the Board must prepare a protected review report that includes the information, see section 54.</li> <li>(2) Sensitive review information is information the disclosure of which:         <ul> <li>(a) could prejudice the security, defence or international relations of Australia; or</li> <li>(b) would prejudice relations between the Commonwealth government and the government of a State or Territory; or</li> <li>(c) could reveal, or enable a person to ascertain, the existence or identity of a confidential source of information in relation to</li> </ul> </li> </ol>

1 2	(e) would prejudice the fair trial of any person or the impartial adjudication of a matter; or
3 4 5	(f) would involve disclosing information whose disclosure is prohibited or restricted by or under this Act, another Act or an instrument made under an Act; or
6 7	<ul> <li>(g) would involve unreasonably disclosing information that is confidential or commercially sensitive; or</li> </ul>
8 9	(h) would involve the disclosure of personal information about an individual without their consent.
10	54 Protected review reports
11 12 13	(1) If information must be redacted from a final review report under section 53, the Board must prepare another report (a <i>protected review report</i> ) that includes:
14	(a) the redacted information; and
15 16	(b) the reasons for redacting the information from the final review report.
17 18 19 20	<ul><li>(2) If a protected review report is prepared under this section, the Board must give the Minister, and the Prime Minister, a copy of:</li><li>(a) the final review report prepared under section 52; and</li><li>(b) a copy of the protected review report.</li></ul>
21 22 23 24	(3) The Minister may give a copy of the protected review report, or ar extract of the protected review report, to any other Commonwealth body, a State body or an entity but only for the purposes of one or more of the following:
25 26 27	<ul> <li>(a) the performance of the functions of a Commonwealth body relating to responding to, mitigating or resolving a cyber security incident;</li> </ul>
28 29 30	<ul> <li>(b) the performance of the functions of a State body relating to responding to, mitigating or resolving a cyber security incident;</li> </ul>
31 32	(c) informing and advising the Minister, and other Ministers of the Commonwealth, about a cyber security incident;
33	(d) the performance of the functions of an intelligence agency.

# **Division 3—Protection of information relating to reviews**

55 Limitations on use and disclosure by the Board	55	<b>Limitations on</b>	use and	disclosure	by the	<b>Board</b>
---	----	-----------------------	---------	------------	--------	--------------

3	55 Limitations on use and disclosure by the Board
4	Permitted use and disclosure
5	(1) The Board may make a record of, use or disclose information
6	provided by an entity, Commonwealth body or State body under
7	section 48, 49 or 51 but only:
8	(a) for the purposes of one or more of the following:
9	(i) performing functions or exercising powers under this
10	Part or Part 6 as it applies to this Part;
11	(ii) proceedings under, or arising out of, section 137.1 or
12	137.2 of the <i>Criminal Code</i> (false and misleading
13	information and documents) that relate to this Act;
14	(iii) proceedings for an offence against section 149.1 of the
15	Criminal Code (which deals with obstruction of
16	Commonwealth public officials) that relates to this Act;
17	(iv) the performance of the functions of a Commonwealth
18	body relating to responding to, mitigating or resolving a
19	cyber security incident;
20	(v) the performance of the functions of a State body relating
21	to responding to, mitigating or resolving a cyber
22	security incident;
23	(vi) informing and advising the Minister, and other
24	Ministers of the Commonwealth, about a cyber security
25	incident;
26	(vii) the performance of the functions of an intelligence
27	agency; or
28	(b) as otherwise authorised by a provision of this Part.
29	Note: Certain information must not be disclosed to a State body under Parts
30	of this Act unless a Minister of the State or Territory has consented to
31	those Parts applying to the State body: see section 11.

1		Restriction on use and disclosure for civil or regulatory action
2 3 4 5	(2)	However, the Board must not make a record of, use or disclose the information for the purposes of investigating or enforcing, or assisting in the investigation or enforcement of, any contravention by the entity or body of a Commonwealth, State or Territory law other than:
7		(a) a contravention by the entity or body of this Part; or
8 9		<ul><li>(b) a contravention by the entity or body of a law that imposes a penalty or sanction for a criminal offence.</li></ul>
10 11		Note: See also section 58 in relation to admissibility of the information in proceedings.
12		Interaction with the Privacy Act 1988
13 14	(3)	Subsection (1) does not authorise the Board to record, use or disclose the information to the extent that it is prohibited or
15		restricted by or under the <i>Privacy Act 1988</i> .
16		Information not covered by the prohibitions in this section
17 18 19	(4)	Subsection (1) does not prohibit the recording, use or disclosure of information that has already been lawfully made available to the public.
20	56 Limita	tions on secondary use and disclosure
21	(1)	This section applies to information that:
22 23		(a) has been provided to the Board under section 48, 49 or 51; and
24 25		(b) has been obtained under section 54 or 55, or this section, by an entity, a Commonwealth body or a State body; and
26		(c) is held by the entity, Commonwealth body or State body.
27 28 29		Note: This section does not apply to the information to the extent that it has been otherwise obtained by the entity, Commonwealth body or State body.

1	Permitted use and disclosure
2 3	(2) The entity, Commonwealth body or State body may make a record of, use or disclose the information but only:
4	(a) for the purposes of one or more of the following:
5	(i) performing functions or exercising powers, or assisting
6	in the performance of functions or the exercise of
7	powers, under this Part or Part 6 as it applies to this
8	Part;
9	(ii) proceedings under, or arising out of, section 137.1 or
0	137.2 of the Criminal Code (false and misleading
1	information and documents) that relate to this Act;
12	(iii) proceedings for an offence against section 149.1 of the
13	Criminal Code (which deals with obstruction of
14	Commonwealth public officials) that relates to this Act;
15	(iv) the performance of the functions of a Commonwealth
16	body relating to responding to, mitigating or resolving a
17	cyber security incident;
8	(v) the performance of the functions of a State body relating
19	to responding to, mitigating or resolving a cyber
20	security incident;
21	(vi) informing and advising the Minister, and other
22	Ministers of the Commonwealth, about a cyber security
23	incident;
24	(vii) the performance of the functions of an intelligence
25	agency; or
26	(b) as otherwise authorised by a provision of this Part.
27	Restriction on use and disclosure for civil or regulatory action
28	(3) However, the entity, Commonwealth body or State body must not
29	make a record of, use or disclose the information for the purposes
30	of investigating or enforcing, or assisting in the investigation or
31	enforcement of, any contravention, by the entity or body that
32	originally provided the information under section 48, 49 or 51, of a
33	Commonwealth, State or Territory law other than:
34	(a) a contravention by the entity or body of this Part; or

1 2	(b) a contravention by the entity or body of a law that imposes a penalty or sanction for a criminal offence.
3 4	Note: See also section 58 in relation to admissibility of the information in proceedings.
5	Interaction with the Privacy Act 1988
6	(4) Subsection (2) does not authorise the entity, Commonwealth body
7	or State body to record, use or disclose the information to the
8	extent that it is prohibited or restricted by or under the Privacy Act
9	1988.
10	Information not covered by the prohibitions in this section
11	(5) Subsection (2) does not prohibit:
12	(a) recording, use or disclosure of information that has already
13	been lawfully made available to the public (for example, in
14	the publication of the final review report); or
15	(b) if the entity is an individual—recording, use or disclosure of
16	personal information about the individual; or
17	(c) if the entity or body is the entity or body that originally
18	provided the information under section 48, 49 or 51—the
19	entity's or body's own information; or
20	(d) recording, use or disclosure of that entity's or body's own
21 22	information, with the consent of that entity or body, by another entity, a Commonwealth body or a State body; or
	(e) recording, use or disclosure of information for the purposes
23 24	of carrying out a State's constitutional functions, powers or
25	duties.
26	Civil penalty for contravention of this section
27	(6) An entity is liable to a civil penalty if:
28	(a) the entity contravenes subsection (2); and
29	(b) the entity is not a Commonwealth officer; and
30	(c) any of the following applies:
31	(i) the information is sensitive information about an
32	individual and the individual has not consented to the
33	record, use or disclosure of the information;

1 2	<ul><li>(ii) the information is confidential or commercially sensitive;</li></ul>
	·
3	(iii) the record, use or disclosure of the information would, or could reasonably be expected to, cause damage to the
4 5	security, defence or international relations of the
6	Commonwealth.
7	Note 1: See the <i>Criminal Code</i> for offences for Commonwealth officers.
8 9	Note 2: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.
10	Civil penalty: 60 penalty units.
11	57 Legal professional privilege
12	(1) The fact that an entity provided information to the Board under
13	section 48, 49 or 51 does not otherwise affect a claim of legal
14	professional privilege that anyone may make in relation to that
15	information in any proceedings:
16	(a) under any Commonwealth, State or Territory law (including
17	the common law); or
18	(b) before a tribunal of the Commonwealth, a State or a
19	Territory.
20	(2) Despite subsection (1), this section does not apply to the following:
21	(a) the proceedings of a coronial inquiry or a Royal Commission
22	in Australia;
23	(b) proceedings in a federal court exercising original jurisdiction
24	in which a writ of mandamus or prohibition or an injunction
25	is sought against an officer or officers of the Commonwealth.
26 27	Note: For <i>federal court</i> , see section 2B of the <i>Acts Interpretation Act</i> 1901.
28	(3) This section does not limit or affect any right, privilege or
29	immunity that the entity has, apart from this section, as a defendant
30	in any proceedings.

1 2	58 Admissibility of information given by an entity that has been requested or required by the Board
3	(1) This section applies to information that:
4 5	(a) has been provided by an entity to the Board under section 48, 49 or 51; and
6 7	(b) has been obtained under section 48, 49, 51, 54, 55 or 56 by a Commonwealth body or a State body; and
8	(c) is held by the Commonwealth body or State body.
9	Note: This section does not apply to information held by the Commonwealth body or State body to the extent that it has been otherwise obtained.
1 1 2	(2) The information is not admissible in evidence against the entity in any of the following proceedings:
13	(a) criminal proceedings for an offence under a Commonwealth law, other than:
15 16 17	(i) proceedings for an offence against section 137.1 or 137.2 of the <i>Criminal Code</i> (which deal with false or misleading information or documents) that relates to this Act; or
19 20 21	<ul><li>(ii) proceedings for an offence against section 149.1 of the Criminal Code (which deals with obstruction of Commonwealth public officials) that relates to this Act;</li></ul>
22 23 24	<ul> <li>(b) civil proceedings for a contravention of a civil penalty provision of a Commonwealth law, other than a civil penalty provision of this Part;</li> </ul>
25 26	(c) proceedings for a breach of any other Commonwealth, State or Territory law (including the common law);
27 28	(d) proceedings before a tribunal of the Commonwealth, a State or a Territory.
29	(4) This section does not apply to the following:
30 31	<ul> <li>(a) the proceedings of a coronial inquiry or a Royal Commission in Australia;</li> </ul>
32 33	(b) proceedings in a federal court exercising original jurisdiction in which a writ of mandamus or prohibition or an injunction is sought against an officer or officers of the Commonwealth
34	is sought against an officer or officers of the Commonwealth

1 2	Note: For <i>federal court</i> , see section 2B of the <i>Acts Interpretation Act</i> 1901.
3	(5) This section does not limit or affect any right, privilege or
4	immunity that the entity has, apart from this section, as a defendant
5	in any proceedings.
6	59 Disclosure of draft review reports prohibited
7	(1) An entity is liable to a civil penalty if:
8	(a) the entity receives a draft review report under section 51; and
9	(b) the entity makes a record of, discloses or otherwise uses any
10	information in the draft review report.
11	Civil penalty: 60 penalty units.
12	(2) Subsection (1) does not apply if the making of the record,
13	disclosure or use is:
14	(a) for the purpose of preparing a submission to the Board in
15	accordance with section 51; or
16	(b) if the entity is the entity that originally provided the
17	information under section 48 or 49—of the entity's own
18	information; or
19	(c) with the consent of the Chair of the Board; or
20	(d) after the information has already been lawfully made
21	available to the public (for example, in the publication of the
22	final review report);
23	(e) for the purposes of carrying out a State's constitutional
24	functions, powers or duties.
25	(3) Despite section 96 of the Regulatory Powers Act, in proceedings
26	for a civil penalty order against an entity for a contravention of
27	subsection (1), the entity does not bear an evidential burden in
28	relation to the matters in subsection (2).
29	Note: This Act does not make the Crown (other than an authority of the
30	Crown) liable to a civil penalty.

1	Division 4—Establishment, functions and powers of the
2	Board
3	60 Cyber Incident Review Board
4	(1) The Cyber Incident Review Board is established by this section.
5 6 7 8	(2) For the purposes of paragraph (a) of the definition of <i>Department</i> of <i>State</i> in section 8 of the <i>Public Governance</i> , <i>Performance and Accountability Act 2013</i> , the Cyber Incident Review Board is prescribed in relation to the Department.
9 10 11	Note: Subject to subsection (2), this means that the chair and members of the Board are officials of the Department for the purposes of the <i>Public Governance, Performance and Accountability Act 2013</i> .
12	61 Constitution of the Board
13	The Board consists of the following members:
4	(a) a Chair;
15	(b) at least 2, and not more than 6, other standing members.
16	62 Functions of the Board
17	(1) The functions of the Board are:
18	(a) to cause reviews to be conducted by review panels in relation
9	to cyber security incidents, or series of related cyber security
20	incidents, to:
21	(i) identify factors that contributed to the incident or series
22	of incidents; and
23	(ii) make recommendations to government and industry
24	about actions that could be taken to prevent, detect,
25 26	respond to or minimise the impact of, incidents of a similar nature in the future; and
27	(iii) report publicly on the review; and
28	(b) any other functions conferred on the Board by this Act or the
28 29	rules.
-/	T WILLOW

1 2		Note: See section 46 in relation to the circumstances in which a cyber security incident may be reviewed.
3	(2)	It is not a function of the Board to:
4		(a) apportion blame in relation to a cyber security incident; or
5		(b) provide the means to determine the liability of any entity in
6		relation to a cyber security incident; or
7 8		(c) allow any adverse inference to be drawn from the fact that are entity is the subject of a review.
9		However, even though blame or liability may be inferred, or an
10		adverse inference may be made, by a person other than the Board,
11		this does not prevent the Board from carrying out its functions.
12	(3)	The Board has power to do all things necessary or convenient to be
13		done for or in connection with the performance of the Board's
14		functions.
15	(4)	The Board must not perform a function or exercise a power under
16		this Part at a particular time if the performance of the function or
17		the exercise of the power at that time would prejudice the
18		investigation of, or the conduct of proceedings relating to, an
19 20		offence or a contravention of a civil penalty provision under a law of the Commonwealth or of a State or Territory.
21	(5)	The rules may prescribe the circumstances in which cyber security
22		incidents are a series of related incidents for the purposes of this
23		section.
24		Note: For example, the rules may prescribe that cyber security incidents are
25		a series of related incidents if the incidents involve a common type of
26		impacted system or a common attack method.
27	63 Indepe	ndence
28		Subject to this Act and to other laws of the Commonwealth, the
29		Cyber Incident Review Board:
30		(a) has complete discretion in the performance of the Board's
31		functions and the exercise of the Board's powers; and
32		(b) is not subject to direction by any person in relation to the
33		performance or exercise of those functions or powers.

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

## Section 63

Note: The Minister must approve the terms of reference for a review to be undertaken by the Board: see subsection 46(2).

1

# Division 5—Terms and conditions of appointment of the Chair and members of the Board

2			Chair and members of the Board
3	64	Appoir	ntment of Chair
4 5		(1)	The Chair of the Board is to be appointed by the Minister by written instrument.
6 7			Note: The Chair may be reappointed: see section 33AA of the <i>Acts Interpretation Act 1901</i> .
8		(2)	The Chair may be appointed on a full-time or part-time basis.
9		(3)	The Chair holds office for the period specified in the instrument of appointment. The period must not exceed 4 years.
1 2		(4)	The rules may make provision for or in relation to the appointment of the Chair, including in relation to eligibility for appointment.
13	65	Remun	neration of the Chair
14 15 16		(1)	The Chair of the Board is to be paid the remuneration that is determined by the Remuneration Tribunal. If no determination of that remuneration by the Tribunal is in operation, the Chair is to be paid the remuneration that is prescribed by the rules.
18		(2)	The Chair is to be paid the allowances that are prescribed by the rules.
20 21		(3)	This section has effect subject to the <i>Remuneration Tribunal Act</i> 1973.
22	66	Appoin	ntment of standing members of the Board
23 24		(1)	A standing member of the Board is to be appointed by the Minister by written instrument.
25 26			Note: A member may be reappointed: see section 33AA of the <i>Acts Interpretation Act 1901</i> .

C4:	$\sim$
Section	n'
Dection	$\mathbf{O}_{I}$

1 2		(2)	A standing member of the Board may be appointed on a full-time or part-time basis.
3 4		(3)	A standing member of the Board holds office for the period specified in the instrument of appointment. The period must not
5			exceed 4 years.
6		(4)	The rules may make provision for or in relation to the appointment
7 8			of standing members of the Board, including in relation to eligibility for appointment.
9	67	Remun	neration of standing members of the Board
10		(1)	A standing member of the Board is to be paid the remuneration that
11			is determined by the Remuneration Tribunal. If no determination of
12 13			that remuneration by the Tribunal is in operation, a standing member of the Board is to be paid the remuneration that is
14			prescribed by the rules.
15		(2)	A standing member of the Board is to be paid the allowances that
16			are prescribed by the rules.
17		(3)	This section has effect subject to the Remuneration Tribunal Act
18			1973.
19	68	Acting	Chair
20			The Minister may, by written instrument, appoint a standing
21			member of the Board to act as the Chair:
22			(a) during a vacancy in the office of Chair (whether or not an
23			appointment has previously been made to the office); or
24			(b) during any period, or during all periods, when the Chair:
25			(i) is absent from duty or from Australia; or
26 27			(ii) is, for any reason, unable to perform the duties of the office.
28 29			Note: For rules that apply to acting appointments, see section 33A of the Acts Interpretation Act 1901.

1	69 Terms and conditions etc. for standing members
2	(1) The rules may make provision for or in relation to the Board,
3	including for or in relation to the following:
4	(a) membership of the Board (subject to section 61);
5	(b) terms of appointment of the Chair and standing members;
6	(c) acting appointments;
7	(d) resignation of the Chair and standing members;
8	(e) disclosure of interests by the Chair and standing members;
9	(f) termination of appointment of the Chair and standing
10	members;
11	(g) leave of absence of the Chair and standing members.
12	(2) The Chair and a standing member of the Board holds office on the
13	terms and conditions (if any) that are determined by the Minister in
14	relation to matters not covered by this Act or the rules.

# Division 6—Expert Panel, staff assisting and consultants

70	Expert	Panel
	(1)	The Board may, in writing, establish an Expert Panel.
	(2)	The Expert Panel consists of such members as the Board from time to time appoints by written instrument.
		Note: A member of the Expert Panel may be reappointed: see section 33AA of the <i>Acts Interpretation Act 1901</i> .
	(3)	One or more members of the Expert Panel are to be appointed by the Board, in writing and in accordance with the terms of reference for a review under section 46, to the review panel for the review to assist in the review.
	(4)	The office of member of the Expert Panel, and the office of member of the Expert Panel assisting in relation to a review, are not public offices within the meaning of the <i>Remuneration Tribunal Act 1973</i> .
	(5)	The rules may make provision for or in relation to the Expert Panel, including for or in relation to the following:  (a) membership of the Expert Panel; (b) appointment of members to the Expert Panel; (c) appointments of its members to a review panel for a review; (d) terms of appointment of members; (e) remuneration of members; (f) resignation of members; (g) disclosure of interests by members; (h) termination of appointment of members; (i) leave of absence of members.
71	Arrang	gements relating to staff of the Department
	(1)	The staff assisting the Cyber Incident Review Board are to be APS employees, or officers or employees of a Commonwealth body, whose services are made available to the Board in connection with

1

2

3

4

5

6

8

9

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

#### 72 Consultants

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

# **Division 7—Other matters relating to the Board**

2	13	Board	procedures
3		(1)	Subject to this Act and the rules, the Board may:
4			(a) operate in the way it determines; and
5			(b) regulate proceedings at its meetings as it considers
6			appropriate.
7		(2)	The rules may make provision for or in relation to the operation
8			and procedures of the Board.
9	74	Liabili	ty
10			Responding to notices to produce
11		(1)	An entity is not liable to an action or other proceeding for damages
12			for or in relation to an act done or omitted in good faith in
13			compliance with section 49 (Chair may obtain documents from
14			certain entities).
15		(2)	An officer, employee or agent of an entity is not liable to an action
16			for damages for or in relation to an act done or omitted in good
17			faith in connection with an act done or omitted by the entity as
18			mentioned in subsection (1).
19			The Board etc.
20		(3)	A person who is or has been:
21			(a) the Chair; or
22			(b) a standing member of the Board; or
23			(c) a member of the Expert Panel; or
24			(d) a member of the staff assisting the Board (as mentioned in
25			section 71); or
26			(e) a consultant assisting the Board (as mentioned in section 72);
27			or
28			(f) a witness appearing in a review;

1 2 3 4 5	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 the performance or purported performance of a function or duty conferred by this Part, or the exercise or purported exercise of a power conferred by this Part.
6	Evidential burden
7 8 9 10	(4) An entity or person who wishes to rely on subsection (1), (2) or (3) in relation to an action or other proceeding bears an evidential burden (within the meaning of the Regulatory Powers Act) in relation to that matter.
11	75 Certification of involvement in review
12 13	(1) The Chair may issue a certificate stating that a specified person who is, or has been:
14	(a) a standing member of the Board; or
15	(b) a member of the Expert Panel; or
16 17	(c) a member of the staff assisting the Board (as mentioned in section 71); or
18 19	(d) a consultant assisting the Board (as mentioned in section 72); or
20	(e) a witness appearing in a review;
21 22	is involved, or has been involved, in a review under this Part into a specified matter.
23 24	(2) The Secretary may issue a certificate stating that a specified person who is, or has been, the Chair is involved, or has been involved, in
25	a review under this Part into a specified matter.
26 27	(3) If, under subsection (1) or (2), a certificate is issued in relation to a person and a specified matter, the person:
28	(a) is not obliged to comply with a subpoena or similar direction
29	of a federal court or a court of a State or Territory to attend
30	and answer questions relating to the matter; and
31	(b) is not compellable to give an expert opinion in any civil or
32 33	criminal proceedings in a federal court or a court of a State or Territory in relation to the matter.

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

#### 76 Annual report 2 The annual report prepared by the Secretary and given to the 3 Minister under section 46 of the Public Governance, Performance 4 and Accountability Act 2013 for a reporting period must also 5 include the following: 6 (a) the number of each of the following during the period: 7 (i) reviews commenced; 8 (ii) reviews completed; 9 (iii) reviews discontinued; 10 (b) a brief description of each of those reviews; 11 (c) the status of any reviews not yet completed at the end of the 12 13 period; (d) the reasons for discontinuing any reviews during the period; 14 (e) the number of times the Minister refused to approve the 15 terms of reference for a review during the period; 16 (f) the number of members of the Expert Panel during the 17 period; 18 (g) the number of Expert Panel members appointed to a review 19 panel during the period; 20 (h) the number of times appointment of a member of the Board 21 was terminated during the period. 22 77 Rules may prescribe reporting requirements etc. 23 The rules may prescribe requirements with which the Board must 24 comply relating to: 2.5 (a) the communication of information to the public; and 26 (b) reporting to the Minister; 27

about the work of the Board.

28

2

3

## Part 6—Regulatory powers

### Division 1—Preliminary

### 78 Simplified outline of this Part

Each civil penalty provision of this Act, and of Division 1A of 4 Part 6 of the *Intelligence Services Act 2001*, is subject to: 5 monitoring under Part 2 of the Regulatory Powers Act; 6 7 investigation under Part 3 of the Regulatory Powers Act. (b) 8 Sections 15 and 16 of this Act (regarding security standards) are also subject to monitoring under Part 2 of the Regulatory Powers 10 Act. 11 Civil penalty orders may be sought under Part 4 of the Regulatory 12 Powers Act from a relevant court in relation to contraventions of 13 such civil penalty provisions. Infringement notices may be given under Part 5 of the Regulatory 15 Powers Act for alleged contraventions of such civil penalty 16 provisions. 17 Undertakings to comply with such civil penalty provisions, and 18 sections 15 and 16 (regarding security standards), may be accepted 19 and enforced under Part 6 of the Regulatory Powers Act. 20 Injunctions under Part 7 of the Regulatory Powers Act may be used 2.1 to restrain a person from contravening, or to compel compliance 22 with, such civil penalty provisions. 23

# Division 2—Civil penalty provisions, enforceable undertakings and injunctions

	under	takings and injunctions
79 Civil p		rovisions, enforceable undertakings and
	mjunce	10115
	Enforce	able provisions
(1)	Each civ	vil penalty provision of this Act, and each civil penalty
		n of Division 1A of Part 6 of the <i>Intelligence Services Act</i>
	2001, is	enforceable:
	(a) un	der Part 4 of the Regulatory Powers Act (civil penalty
	pre	ovisions); and
	(b) Pa	rt 7 (injunctions) of the Regulatory Powers Act.
	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 7 of that Act creates a framework for using injunctions to enforce provisions.
(2)	The foll	owing provisions are enforceable under Part 6 (enforceable
	undertak	kings) of the Regulatory Powers Act:
	(a) ea	ch civil penalty provision of this Act, and each civil
	pe	nalty provision of Division 1A of Part 6 of the <i>Intelligence</i>
	Se	rvices Act 2001;
	(b) see	ctions 15 and 16 of this Act.
	Note:	Part 6 of the Regulatory Powers Act creates a framework for
		accepting and enforcing undertakings relating to compliance with
		provisions.
	Authoris	sed applicant
(3)	For the j	purposes of Parts 4 and 7 of the Regulatory Powers Act,
		the following persons is an authorised applicant in relation
	to the ci	vil penalty provisions mentioned in subsection (1):
	(a) the	e Secretary;
	(b) a p	person who is appointed under subsection (4).
	(2)	79 Civil penalty pinjunct  Enforced  (1) Each civil provision 2001, is  (a) unil provision 2001.  (b) Part Note 1:  Note 2:  (2) The followindertake (a) each person of to the civil circle of the cir

1 2	(4) For the purposes of paragraph (3)(b), the Secretary may, by writing, appoint a person who:
3	(a) is the chief executive officer (however described) of a designated Commonwealth body; or
5	(b) is an SES employee, or an acting SES employee, in:
	(i) the Department; or
6 7	(ii) a designated Commonwealth body; or
	(c) holds, or is acting in, a position in a designated
8 9	Commonwealth body that is equivalent to, or higher than, a
10	position occupied by an SES employee;
11 12	to be an authorised applicant for the purposes of Part 4 of the Regulatory Powers Act.
13 14	Note: The expressions <b>SES employee</b> and <b>acting SES employee</b> are defined in section 2B of the <b>Acts Interpretation Act 1901</b> .
15	Authorised person
16	(5) For the purposes of Part 6 of the Regulatory Powers Act, as that
17	Part applies in relation to a provision mentioned in subsection (2),
18	each of the following persons is an authorised person:
19	(a) the Secretary;
20	(b) a person who is appointed under subsection (6).
21	(6) For the purposes of paragraph (5)(b), the Secretary may, by
22	writing, appoint a person who is an SES employee, or an acting
23	SES employee in:
24	(a) the Department; or
25	(b) a designated Commonwealth body.
26 27	Note: The expressions <b>SES employee</b> and <b>acting SES employee</b> are defined in section 2B of the <b>Acts Interpretation Act 1901</b> .
28	Relevant court
29	(7) For the purposes of Parts 4, 6 and 7 of the Regulatory Powers Act,
30	each of the following courts is a relevant court in relation to the
31	provisions mentioned in subsections (1) and (2):
32	(a) the Federal Court of Australia;

1	(b) the Federal Circuit and Family Court of Australia
2	(Division 2);
3	(c) a court of a State or Territory that has jurisdiction in relation
4	to the matter.
5	Liability of Crown
6	(8) Part 4 of the Regulatory Powers Act, as that Part applies in relation
7	to the civil penalty provisions mentioned in subsection (1), does
8	not make the Crown liable to a pecuniary penalty.
9	(9) The protection in subsection (8) does not apply to an authority of
10	the Crown.

1

2

# Division 3—Monitoring and investigation powers

$\alpha$	TA #
XU	<b>Monitoring powers</b>
OU	months powers

3	Provisions subject to monitoring
4	(1) The following provisions are subject to monitoring under Part 2 of
5	the Regulatory Powers Act:
6	(a) each civil penalty provision of this Act;
7 8	(b) each civil penalty provision of Division 1A of Part 6 of the <i>Intelligence Services Act 2001</i> ;
9	(c) sections 15 and 16 of this Act.
10 11 12	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.
13	Information subject to monitoring
14	(2) Information given in compliance or purported compliance with a
15 16	provision mentioned in subsection (1) is subject to monitoring under Part 2 of the Regulatory Powers Act.
	Ç
17 18	Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether the information is correct. It includes powers of
19	entry and inspection.
20	Authorised applicant
21	(3) For the purposes of Part 2 of the Regulatory Powers Act, a person
22	who is appointed under subsection (4) is an authorised applicant in
23	relation to the provisions mentioned in subsection (1) and
24	information mentioned in subsection (2).
25	(4) The Secretary may, by writing, appoint a person who:
26	(a) is an SES employee, or an acting SES employee, in:
27	(i) the Department; or
28	(ii) a designated Commonwealth body; or

1 2 3	(b) holds, or is acting in, a position in a designated Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee;
4 5 6	to be an authorised applicant in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).
7 8	Note: The expressions <i>SES employee</i> and <i>acting SES employee</i> are defined in section 2B of the <i>Acts Interpretation Act 1901</i> .
9	Authorised person
10 11 12	(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
13	information mentioned in subsection (2).
14	(6) The Secretary may, by writing, appoint a person who is:
15	(a) an APS employee in:
16	(i) the Department; or
17	(ii) a designated Commonwealth body; or
18	(b) an officer or employee of a designated Commonwealth body;
19 20	to be an authorised person in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).
21	Issuing officer
22	(7) For the purposes of Part 2 of the Regulatory Powers Act, a
23	magistrate is an issuing officer in relation to the provisions
24	mentioned in subsection (1) and information mentioned in
25	subsection (2).
26	Relevant chief executive
27	(8) For the purposes of Part 2 of the Regulatory Powers Act, the
28	Secretary is the relevant chief executive in relation to the
29	provisions mentioned in subsection (1) and information mentioned
30	in subsection (2).

	Relevant court
(9)	For the purposes of Part 2 of the Regulatory Powers Act, each of
	the following courts is a relevant court in relation to the provisions
	mentioned in subsection (1) and information mentioned in
	subsection (2):
	(a) the Federal Court of Australia;
	(b) the Federal Circuit and Family Court of Australia
	(Division 2);
	(c) a court of a State or Territory that has jurisdiction in relation
	to matters arising under this Act.
	Premises
(10)	An authorised person must not enter premises under Part 2 of the
( - /	Regulatory Powers Act, as it applies in relation to the provisions
	mentioned in subsection (1) and information mentioned in
	subsection (2), if the premises are used solely or primarily as a
	residence.
81 Investi	gation powers
	Provisions subject to investigation
(1)	Each civil penalty provision of this Act, and each civil penalty
(1)	provision of Division 1A of Part 6 of the <i>Intelligence Services Act</i>
	2001, is subject to investigation under Part 3 of the Regulatory
	Powers 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:
(3)	The Secretary may, by writing, appoint a person who:  (a) is an SES employee, or an acting SES employee, in:
(3)	(a) is an SES employee, or an acting SES employee, in:
(3)	
	(10)  81 Investi

1 2 3	<ul> <li>(b) holds, or is acting in, a position in a designated</li> <li>Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee;</li> </ul>
4 5	to be an authorised applicant in relation to evidential material that relates to a provision mentioned in subsection (1).
6 7	Note: The expressions <i>SES employee</i> and <i>acting SES employee</i> are defined in section 2B of the <i>Acts Interpretation Act 1901</i> .
8	Authorised person
9	(4) For the purposes of Part 3 of the Regulatory Powers Act, a person
10	who is appointed under subsection (5) is an authorised person in
11 12	relation to evidential material that relates to a provision mentioned in subsection (1).
13	(5) The Secretary may, by writing, appoint a person who is:
14	(a) an APS employee in:
15	(i) the Department; or
16	(ii) a designated Commonwealth body; or
17	(b) an officer or employee of a designated Commonwealth body;
18	to be an authorised person in relation to evidential material that
19	relates to a provision mentioned in subsection (1).
20	Issuing officer
21	(6) For the purposes of Part 3 of the Regulatory Powers Act, a
22	magistrate is an issuing officer in relation to evidential material
23	that relates to a provision mentioned in subsection (1).
24	Relevant chief executive
25	(7) For the purposes of Part 3 of the Regulatory Powers Act, the
26	Secretary is the relevant chief executive in relation to evidential
27	material that relates to a provision mentioned in subsection (1).
28	Relevant court
29	(8) For the purposes of Part 3 of the Regulatory Powers Act, each of
30	the following courts is a relevant court in relation to evidential
31	material that relates to a provision mentioned in subsection (1):

# Part 6 Regulatory powersDivision 3 Monitoring and investigation powers

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

# **Division 4—Infringement notices**

## **82 Infringement notices**

3	Provisions subject to an infringement notice
4	(1) A civil penalty provision of this Act or of Division 1A of Part 6 of
5	the Intelligence Services Act 2001 is subject to an infringement
6	notice under Part 5 of the Regulatory Powers Act.
7 8	Note: Part 5 of the Regulatory Powers Act creates a framework for using infringement notices in relation to provisions.
9	Infringement officer
10	(2) For the purposes of Part 5 of the Regulatory Powers Act, a person
11	authorised under subsection (3) is an infringement officer in
12	relation to the civil penalty provisions mentioned in subsection (1).
13	(3) The Secretary may, by writing, authorise a person who:
14	(a) is an SES employee, or an acting SES employee, in:
15	(i) the Department; or
16	(ii) a designated Commonwealth body; or
	(b) holds, or is acting in, a position in a designated
17 18	Commonwealth body that is equivalent to, or higher than, a
19	position occupied by an SES employee;
	to be an infringement officer in relation to the civil penalty
20 21	provisions mentioned in subsection (1).
22	Note: The expressions <b>SES employee</b> and <b>acting SES employee</b> are defined
23	in section 2B of the Acts Interpretation Act 1901.
24	Relevant chief executive
25	(4) For the purposes of Part 5 of the Regulatory Powers Act, the
26	Secretary is the relevant chief executive in relation to the civil
27	penalty provisions mentioned in subsection (1).
28	(5) The relevant chief executive may, in writing, delegate any or all of
29	the relevant chief executive's powers and functions under Part 5 of

# Part 6 Regulatory powers Division 4 Infringement notices

1	the Regulatory Powers Act to a person who is an SES employee or		
2	an acting SES employee in:		
3	(a) the Department; or		
4	(b) a designated Commonwealth body.		
5 6	Note: The expressions <i>SES employee</i> and <i>acting SES employee</i> are defined in section 2B of the <i>Acts Interpretation Act 1901</i> .		
7	(6) A person exercising powers or performing functions under a		
8	delegation under subsection (5) must comply with any directions of		
9	the relevant chief executive.		
10	Liability of Crown		
1	(7) Part 5 of the Regulatory Powers Act, as that Part applies in relation		
12	to the civil penalty provisions mentioned in subsection (1), does		
13	not make the Crown liable to be given an infringement notice.		
4	(8) The protection in subsection (7) does not apply to an authority of		
15	the Crown.		

### **Division 5—Other matters**

1

2

3

4

5

6

7

8

9

### 83 Contravening a civil penalty provision

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

2

3

4 5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

2.1

22

23

24

25

2627

28

29

# Part 7—Miscellaneous

24	Simn	lifiad	outline	of this	Dart
04	2111111	ımea	outime	OI LIIIS	ran

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

### 85 How this Act applies in relation to non-legal persons

How permissions and rights are conferred and exercised

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

How obligations and duties are imposed and discharged

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

1	How	non-legal persons contravene this Act
2	(3) A pro	ovision of this Act (including a civil penalty provision) that is
3		ortedly contravened by an entity that is not a legal person is
4	instea	ad contravened by each accountable person for the entity who:
5	(a)	did the relevant act or made the relevant omission; or
6	(b)	aided, abetted, counselled or procured the relevant act or
7		omission; or
8	(c)	was in any way knowingly concerned in, or party to, the
9		relevant act or omission.
10	Mear	ning of accountable person
11		the purposes of this section, a person is an <i>accountable person</i>
12		n entity at a particular time if:
13	(a)	in the case of a partnership in which one or more of the
14		partners is an individual—the individual is a partner in the partnership at that time; or
15	(1-)	
16	(0)	in the case of a partnership in which one or more of the partners is a body corporate—the person is a director of the
17 18		body corporate at that time; or
19	(c)	in the case of a trust in which the trustee, or one or more of
20		the trustees, is an individual—the individual is a trustee of
21		the trust at that time; or
22	(d)	in the case of a trust in which the trustee, or one or more of
23		the trustees, is a body corporate—the person is a director of
24		the body corporate at that time; or
25	(e)	in the case of an unincorporated association—the person is a
26		member of the governing body of the unincorporated
27		association at that time.
28	86 Delegation b	by Secretary
29	(1) The S	Secretary may, in writing, delegate all or any of the
30		etary's functions or powers under section 17, 18, 19, 21 or 23
31		SES employee, or acting SES employee, in the Department.
32	Note 1	
33		provisions relating to delegations.

1 2		Note 2: The expressions <i>SES employee</i> and <i>acting SES employee</i> are defined in section 2B of the <i>Acts Interpretation Act 1901</i> .
3	(2)	In performing a delegated function or exercising a delegated
4	` ,	power, the delegate must comply with any written directions of the
5		Secretary.
6	87 Rules	
7	(1)	The Minister may, by legislative instrument, make rules
8		prescribing matters:
9 10		(a) required or permitted by this Act to be prescribed by the rules; or
11		(b) necessary or convenient to be prescribed for carrying out or
12		giving effect to this Act.
13	(2)	To avoid doubt, the rules may not do the following:
14		(a) create an offence or civil penalty;
15		(b) provide powers of:
16		(i) arrest or detention; or
17		(ii) entry, search or seizure;
18		(c) impose a tax;
19		(d) set an amount to be appropriated from the Consolidated
20		Revenue Fund under an appropriation in this Act;
21		(e) directly amend the text of this Act.
22	(3)	Before making or amending the rules, the Minister must:
23		(a) cause to be published on the Department's website a notice:
24		(i) setting out the draft rules or amendments; and
25		(ii) inviting persons to make submissions to the Minister
26		about the draft rules or amendments within the period
27		specified in the notice; and
28		(b) consider any submissions received within the period
29		mentioned in subparagraph (a)(ii).
30	(4)	The period specified in the notice must not be shorter than 28 days.

	88 Review of this Act
2	The Parliamentary Joint Committee on Intelligence and Security
3	may:
ļ 5	(a) review the operation, effectiveness and implications of this Act; and
5	(b) report the Committee's comments and recommendations to each House of the Parliament;
3	so long as the Committee begins the review as soon as practicable
)	after 1 December 2027.

10

(116/24)