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

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

The Parliament of Australia enacts:

Part 1—Preliminary

1 Short title

This Act is the *Cyber Security Act 2024*.

2 Commencement

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

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

Commencement information

Column 1 Provisions	Column 2 Commencement	Column 3 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Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

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

3 Objects

The objects of this Act are to:

(a) improve the cyber security of products that:

(i) can connect directly or indirectly to the internet; and

(ii) will be acquired in Australia;

by requiring manufacturers and suppliers of those products to comply with security standards specified in the rules; and

(b) encourage the provision of information relating to the provision of payments or benefits (called ransomware payments) to entities seeking to benefit from cyber security incidents by imposing reporting obligations on entities in relation to the payment of such payments or benefits; and

(c) facilitate the whole of Government response to significant cyber security incidents by providing for the National Cyber Security Coordinator to lead across the whole of Government the coordination and triaging of action in response to significant cyber security incidents; and

(d) prevent, improve the detection of, improve the response to and minimise the impact of cyber security incidents by establishing the Cyber Incident Review Board to:

(i) cause reviews to be conducted in relation to certain cyber security incidents; and

(ii) make recommendations to government and industry about actions that could be taken to prevent, detect, respond to or minimise the impact of, incidents of a similar nature in the future; and

(e) improve the response to and minimise the impact of cyber security incidents (including imminent incidents) through encouraging entities impacted, or probably impacted, by such cyber security incidents to provide information to the Australian Government about the incidents by ensuring that:

(i) the information provided is only used and disclosed for limited purposes; and

(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.

A range of compliance and enforcement powers are provided for, including by applying the *Regulatory Powers (Standard Provisions) Act 2014*.

This Act also deals with administrative matters such as delegations and the power to make rules.

5 Extraterritoriality

This Act applies both within and outside Australia.

Note: This Act extends to every external Territory.

6 Act binds the Crown

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

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

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.

7 Concurrent operation of State and Territory laws

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

8 Definitions

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*.

Chair means the Chair of the Cyber Incident Review Board.

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

Commonwealth body means:

(a) a Minister of the Commonwealth; or

(b) a Department of State of the Commonwealth; or

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

(i) is established, or continued in existence, for a public purpose by or under a law of the Commonwealth; and

(ii) is not an authority of the Crown.

Commonwealth enforcement body means:

(a) the Australian Federal Police; or

(b) the Australian Prudential Regulation Authority; or

(c) the Australian Securities and Investments Commission; or

(d) the Inspector of the National Anti-Corruption Commission; or

(e) the Office of the Director of Public Prosecutions; or

(f) the National Anti-Corruption Commissioner; or

(g) Sport Integrity Australia; or

(h) another Commonwealth body, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction for a criminal offence.

Commonwealth officer has the same meaning as in Part 5.6 of the *Criminal Code*.

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

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

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

Cyber Incident Review Board or ***Board*** means the Cyber Incident Review Board established by section 60.

cyber security incident has the meaning given by section 9.

designated Commonwealth body means:

(a) a Department, or a body established by a law of the Commonwealth, specified in the rules; or

(b) if no rules are made for the purposes of paragraph (a)—the Department and ASD.

draft review report has the meaning given by subsection 51(1).

entity means any of the following:

(a) an individual;

(b) a body corporate;

(c) a partnership;

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

(e) a trust;

(f) an entity that is a responsible entity for a critical infrastructure asset.

Expert Panel means the Expert Panel established by the Board under section 70.

final review report has the meaning given by subsection 52(1).

intelligence agency means:

(a) the agency known as the Australian Criminal Intelligence Commission established by the *Australian Crime Commission Act 2002*; or

(b) the Australian Geospatial-Intelligence Organisation; or

(c) the Australian Secret Intelligence Service; or

(d) the Australian Security Intelligence Organisation; or

(e) ASD; or

(f) the Defence Intelligence Organisation; or

(g) the Office of National Intelligence.

internet-connectable product has the meaning given by subsection 13(4).

manufacturer has the same meaning as in the Australian Consumer Law.

National Cyber Security Coordinator means:

(a) the officer of the Department known as the National Cyber Security Coordinator; and

(b) the APS employees, and officers or employees of Commonwealth bodies, whose services are made available to the officer in connection with the performance of any of the officer's functions or the exercise of any of the officer's powers under this Act.

network-connectable product has the meaning given by subsection 13(5).

permitted cyber security purpose for a cyber security incident has the meaning given by section 10.

personal information has the same meaning as in the *Privacy Act 1988*.

protected review report has the meaning given by subsection 54(1).

ransomware payment has the meaning given by subsection 26(1).

ransomware payment report means a report given by an entity under subsection 27(1).

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

relevant connectable product has the meaning given by subsection 13(2).

reporting business entity has the meaning given by subsection 26(2).

responsible entity, for an asset, has the same meaning as in the *Security of Critical Infrastructure Act 2018*.

Secretary means the Secretary of the Department.

sensitive information has the same meaning as in the *Privacy Act 1988*.

sensitive review information has the meaning given by subsection 53(2).

significant cyber security incident has the meaning given by section 34.

State body means:

(a) a Minister of a State or Territory; or

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

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

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

(ii) is not an authority of the Crown.

supply has the same meaning as in the Australian Consumer Law and ***supplied*** and ***supplier*** have corresponding meanings.

9 Meaning of *cyber security incident*

(1) A ***cyber security incident*** is one or more acts, events or circumstances:

(a) of a kind covered by the meaning of ***cyber security incident*** in the *Security of Critical Infrastructure Act 2018*; or

(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.

(2) However, an incident is only a ***cyber security incident*** for the purposes of this Act if:

(a) the incident involves a critical infrastructure asset; or

(b) the incident involves the activities of an entity that is a corporation to which paragraph 51(xx) of the Constitution applies; or

(c) the incident is or was effected by means of a telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution (including, for example, by means of the internet); or

(d) the incident is impeding or impairing, or has impeded or impaired, the ability of a computer to connect to such a service; or

(e) the incident has seriously prejudiced or is seriously prejudicing:

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

(ii) the defence of Australia; or

(iii) national security.

10 Meaning of *permitted cyber security purpose*

Each of the following is a ***permitted cyber security purpose*** for a cyber security incident:

(a) the performance of the functions of a Commonwealth body (to the extent that it is not a Commonwealth enforcement body) relating to responding to, mitigating or resolving the cyber security incident;

(b) the performance of the functions of a State body relating to responding to, mitigating or resolving the cyber security incident;

(c) the performance of the functions of the National Cyber Security Coordinator under Part 4 relating to the cyber security incident;

(d) informing and advising the Minister, and other Ministers of the Commonwealth, about the cyber security incident;

(e) preventing or mitigating material risks that the cyber security 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;

(f) preventing or mitigating material risks to a critical infrastructure asset;

(g) the performance of the functions of an intelligence agency;

(h) the performance of the functions of a Commonwealth enforcement body.

Note 1: There are some limitations in relation to civil or regulatory functions against entities that have provided information in relation to the incident: see subsections 38(2) and 39(3).

Note 2: Certain information must not be disclosed to a State body under Parts of this Act unless a Minister of the State or Territory has consented to those Parts applying to the State body: see section 11.

11 Disclosure to State body

(1) Despite any other provision of this Act, information that may be disclosed to a State body under Part 3, 4 or 5 must not be disclosed to the State body under that Part unless:

(a) a Minister of the State or Territory has informed the Minister administering this Act, in writing, that the State or Territory gives consent to the provisions of that Part applying to the State body; and

(b) a Minister of the State or Territory has not informed the Minister administering this Act, in writing, that the State or Territory withdraws that consent.

(2) For the purposes of paragraph (1)(a), a Minister of a State or Territory may give consent in relation to all State bodies, a class of State bodies, or particular State bodies, of that State or Territory.

Part 2—Security standards for smart devices

Division 1—Preliminary

12 Simplified outline of this Part

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

If the rules provide a security standard for a product:

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

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

An independent audit of a product may be undertaken to determine compliance with the requirements of a security standard or requirements for the statement of compliance. The Secretary may

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

13 Application of this Part

(1) This Part applies to a relevant connectable product that is:

(a) manufactured on or after the commencement of this Part; or

(b) supplied (other than as second hand goods) on or after the commencement of this Part.

(2) A ***relevant connectable product*** is a product that:

(a) is an internet-connectable product or a network-connectable product; and

(b) is not exempted under the rules.

(3) For the purposes of paragraph (2)(b), the rules may specify that:

(a) classes of products are exempted; or

(b) particular products are exempted.

(4) An ***internet-connectable product*** is a product that is capable of connecting to the internet using a communication protocol that forms part of the internet protocol suite to send and receive data over the internet.

(5) A ***network-connectable product*** is a product that:

(a) is capable of both sending and receiving data by means of a transmission involving electrical or electromagnetic energy; and

(b) is not an internet-connectable product; and

(c) meets the condition in subsection (6) or (7).

(6) A product meets the condition in this subsection if it is capable of connecting directly to an internet-connectable product by means of a communication protocol that forms part of the internet protocol suite.

(7) Subject to subsections (8) and (9), a product meets the condition in this subsection if:

(a) it is capable of connecting directly to 2 or more products at the same time by means of a communication protocol that does not form part of the internet protocol suite; and

(b) it is capable of connecting directly to an internet-connectable product by means of such a communication protocol (whether or not at the same time as it connects to any other product).

(8) A product consisting of a wire or cable that is used merely to connect the product to another product does not meet the condition in subsection (7).

(9) If:

(a) two or more products are designed to be used together for the purposes of facilitating the use of a computer (within the ordinary meaning of that expression); and

(b) at least one of the products (the ***linking product***) is capable of connecting directly to an internet-connectable product (whether the computer or some other product) by means of a communication protocol that does not form part of the internet protocol suite; and

(c) each of the products (the ***input products***) that is not a linking product is capable of connecting directly to the linking product, or, if there is more than one linking product, to each linking product:

(i) wirelessly; and

(ii) by means of a communication protocol that does not form part of the internet protocol suite;

each of the input products meets the condition in subsection (7).

(10) For the purposes of subsections (4) to (9), a product is not prevented from being regarded as connecting directly to another product merely because the connection involves the use of a wire or cable.

Division 2—Security standards for relevant connectable products

14 Security standards for relevant connectable products

(1) The rules may make provision for, or in relation to, security standards for specified classes of relevant connectable products that will be acquired in Australia in specified circumstances.

(2) Without limiting subsection (1) a class of relevant connectable products specified for the purposes of that subsection may consist of a particular relevant connectable product or of all relevant connectable products.

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

15 Compliance with security standard for a relevant connectable product

Manufacturer must comply

(1) An entity must manufacture a relevant connectable product in compliance with the requirements of the security standard for a class of relevant connectable product that will be acquired in Australia in specified circumstances if:

(a) the product is included in that class; and

(b) the entity is aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in those circumstances.

(2) The entity must comply with any other requirements of the security standard that apply to the manufacturer of a product included in that class.

(3) An entity must not supply a product in Australia that was not manufactured in compliance with the requirements of the security standard for a class of relevant connectable product that will be acquired in Australia in specified circumstances if:

(a) the product is included in that class; and

(b) the entity is aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in those circumstances.

(4) The entity must comply with any other requirements of the security standard that apply to the supplier of a product included in that class.

Exception

(5) However, to the extent that a requirement in the security standard does not relate to any of the matters in subsection (6), an entity is not required to comply with subsections (1) to (4) if the entity is not:

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

(b) an entity that is undertaking activities in the course of, or in relation to, trade or commerce with other countries, among the States, between Territories or between a Territory and a State.

(6) The matters are the following:

(a) the direct, or indirect, connection of the relevant connectable product to, a telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution (including, for example, connection to the internet);

(b) the direct, or indirect, use by the relevant connectable product of such a service (including, for example, use of the internet);

(c) measures that would protect the relevant connectable product from an attack effected by means of such a service (including, for example, by means of the internet).

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

Manufacturer must provide statement of compliance

(1) An entity that manufactures a relevant connectable product must provide, for the supply of the product in Australia, a statement of compliance with the security standard for a class of relevant connectable product that will be acquired in Australia in specified circumstances if:

(a) the product is included in that class; and

(b) the entity is aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in those circumstances.

(2) The entity must retain a copy of the statement of compliance for the period specified in the rules for that class of statements.

Supplier must supply the product with statement of compliance

(3) An entity that supplies a relevant connectable product in Australia must supply the product with a statement of compliance with the security standard for a class of relevant connectable product that will be acquired in Australia in specified circumstances if:

(a) the product is included in that class; and

(b) the entity is aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in those circumstances.

(4) The entity must retain a copy of the statement of compliance for the period specified in the rules for that class of statements.

Requirements for statement of compliance

(5) The statement of compliance with the security standard under subsection (1) or (2) must meet the requirements provided by the rules for that class of statements.

Matters relating to the rule 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

17 Compliance notice

(1) The Secretary may give an entity that must comply with an obligation under section 15 or 16 a compliance notice if the Secretary:

(a) is reasonably satisfied that the entity is not complying with the obligation; or

(b) is aware of information that suggests that the entity may not be complying with the obligation.

(2) The compliance notice must:

(a) set out the name of the entity to which the notice is given; and

(b) set out brief details of the non-compliance or possible non-compliance; and

(c) specify action within the entity's control that the entity must take in order to address the non-compliance or possible non-compliance; and

(d) specify a reasonable period within which the entity must take the specified action; and

(e) if the Secretary considers it appropriate—specify a reasonable period within which the entity must provide the Secretary with evidence that the entity has taken the specified action; and

(f) explain what may happen if the entity does not comply with the notice; and

(g) explain how the entity may seek review of the decision to issue the notice; and

(h) set out any other matters prescribed by the rules.

(3) Before giving the notice to the entity, the Secretary must:

(a) notify the entity that the Secretary intends to give the notice to the entity; and

(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) Only one compliance notice may be given to an entity in relation to a particular instance of the entity's non-compliance, or possible non-compliance, with an obligation under section 15 or 16.

18 Stop notice

(1) The Secretary may give an entity that must comply with an obligation under section 15 or 16 a stop notice if:

(a) the entity has been given a compliance notice under section 17 in relation to the non-compliance with the obligation; and

(b) the Secretary is reasonably satisfied that:

(i) the entity has not complied with the compliance notice; or

(ii) actions taken by the entity to rectify non-compliance with the obligation (whether in accordance with the compliance notice or otherwise) are inadequate to rectify the non-compliance.

(2) The stop notice must:

(a) set out the name of the entity to which the notice is given; and

(b) set out brief details of the non-compliance; and

(c) specify action within the entity's control that the entity must take, or refrain from taking, in order to address the non-compliance; and

(d) specify a reasonable period within which the entity must take the specified action or refrain from taking the specified action; and

(e) if the Secretary considers it appropriate—specify a reasonable period within which the entity must provide the Secretary with evidence that the entity has taken the specified action or refrained from taking the specified action; and

(f) explain what may happen if the entity does not comply with the notice; and

(g) explain how the entity may seek review of the decision to issue the notice; and

(h) set out any other matters prescribed by the rules.

(3) Before giving the notice to the entity, the Secretary must:

(a) notify the entity that the Secretary intends to give the notice to the entity; and

(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) Only one stop notice may be given to an entity in relation to a particular instance of the entity's non-compliance with an obligation under section 15 or 16.

19 Recall notice

(1) The Secretary may give an entity that must comply with an obligation under section 15 or 16 a recall notice if:

(a) the entity has been given a stop notice under section 18 in relation to the non-compliance with the obligation; and

(b) the Secretary is reasonably satisfied that:

(i) the entity has not complied with the stop notice; or

(ii) actions taken by the entity to rectify the non-compliance with the obligation (whether in accordance with the compliance notice or otherwise) are inadequate to rectify the non-compliance.

(2) The recall notice must:

(a) set out the name of the entity to which the notice is given; and

(b) set out brief details of the non-compliance; and

(c) specify action that the entity must take to do any or all of the following:

(i) ensure, to the extent within the entity's control, the product is not acquired in Australia;

(ii) ensure, to the extent within the entity's control, that the product is not supplied to suppliers for supply in Australia;

(iii) arrange for the return, within a specified reasonable period, of the product to the entity, or if the entity is not the manufacturer of the product, the manufacturer of the product; and

(d) specify a reasonable period within which the entity must take the specified action; and

(e) if the Secretary considers it appropriate—specify a reasonable period within which the entity must provide the Secretary with evidence that the entity has taken the specified action; and

(f) explain what may happen if the entity does not comply with the notice; and

(g) explain how the entity may seek review of the decision to issue the notice; and

(h) set out any other matters prescribed by the rules.

(3) Before giving the notice to the entity, the Secretary must:

(a) notify the entity that the Secretary intends to give the notice to the entity; and

(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) Only one recall notice may be given to an entity in relation to a particular instance of the entity's non-compliance with an obligation under section 15 or 16.

20 Public notification of failure to comply with recall notice

If an entity fails to comply with a recall notice, the Minister may publish the following information on the Department's website, or in any other way the Minister considers appropriate:

(a) the identity of the entity;

(b) details of the product;

(c) details of the non-compliance;

(d) risks posed by the product relating to the non-compliance;

(e) any other matters prescribed by the rules.

Division 4—Miscellaneous

21 Revocation and variation of notices given under this Part

Variation

(1) The Secretary may, by notice in writing given to an entity, vary a compliance notice, stop notice or recall notice given under this Part to the entity if the Secretary is reasonably satisfied that the variation is required:

(a) in order to rectify an error, defect or ambiguity in the notice; or

(b) to adequately rectify the non-compliance, or possible non-compliance, to which the notice relates.

(2) Before giving the notice to the entity under subsection (1), the Secretary must:

(a) notify the entity that the Secretary intends to give the notice to the entity; and

(b) give the entity a specified period (which must not be shorter than 10 days) to make representations about the giving of the notice.

(3) A varied compliance notice, stop notice or recall notice has the same effect as the original notice for the purposes of this Part.

Revocation

(4) The Secretary may, by notice in writing given to an entity, revoke a compliance notice, stop notice or recall notice given under this Part to the entity if the Secretary is no longer satisfied that the grounds for issuing the notice were met.

(5) If a compliance notice, stop notice or recall notice, relating to non-compliance or possible non-compliance by an entity with an obligation, is revoked under subsection (4), no further notices may be issued under this Part in relation to that non-compliance.

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

(1) An entity may apply, in writing, to the Secretary for review (an ***internal review***) of a decision:

(a) to give the entity a compliance notice under section 17; or

(b) to give the entity a stop notice under section 18; or

(c) to give the entity a recall notice under section 19; or

(d) to vary, under section 21, a notice given to the entity.

(2) An application for an internal review must be made within 30 days after the day on which the notice was given to the entity.

(3) The decision-maker for the internal review is:

(a) the Secretary; or

(b) if the Secretary made the decision personally—a person:

(i) to whom the power to issue a notice of that kind has been delegated under section 86; and

(ii) that was not involved in the making of the Secretary's decision.

(4) Within 30 days after the application is received, the decision-maker must:

(a) review the decision; and

(b) affirm, vary or revoke the decision; and

(c) if the decision is revoked—make such other decision (if any) that the decision-maker thinks appropriate.

(5) The decision-maker for the reviewable decision must, as soon as practicable after making a decision under subsection (4), give the applicant a written statement of the decision-maker's reasons for the decision.

23 Examination to assess compliance with security standard and statement of compliance

(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

out an independent examination of the product to determine either or both of the following:

(a) whether the product complies with the security standard for the class of relevant connectable product;

(b) whether the statement of compliance for the product complies with the requirements of section 16.

(2) The expert may examine the product, for example, by doing any of the following:

(a) opening any package in which the product is contained;

(b) operating the product;

(c) testing or analysing the product, including through the use of electronic equipment;

(d) if the product contains a record or document—reading the record or document either directly or with the use of an electronic device;

(e) taking photographs or video recordings of the product.

Request for product and statement of compliance

(3) For the purposes of the examination, the Secretary may request, by notice in writing, the entity to provide the product, or the statement of compliance for the product, or both.

(4) The notice must:

(a) specify the product; and

(b) if the entity is not the manufacturer—specify the manufacturer of the product (if known); and

(c) specify a reasonable period within which the entity must provide the notice; and

(d) specify the period for which the product will be retained for testing; and

(e) specify the requirements of the security standard that the product will be tested against; and

(f) explain the kind of testing or analysis that will be done; and

(g) explain what may happen if:

(i) the entity does not comply with the notice; or

(ii) the entity does not comply with its obligations in section 15 or 16 in relation to the product; and

(h) set out any other matters prescribed by the rules.

Compensation

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

24 Acquisition of property

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

Part 3—Ransomware reporting obligations

Division 1—Preliminary

25 Simplified outline of this Part

This Part imposes reporting obligations on certain entities who are impacted by a cyber security incident, and who have provided or are aware that another entity has provided, a payment or benefit (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 report, including information relating to the cyber security incident, the demand made by the extorting entity and the ransomware payment.

An entity may be liable to a civil penalty if the entity fails to make a ransomware payment report as required by this Part.

Division 2—Reporting obligations

26 Application of this Part

(1) This Part applies if:

(a) an incident has occurred, is occurring or is imminent; and

(b) the incident is a cyber security incident; and

(c) the incident has had, is having, or could reasonably be expected to have, a direct or indirect impact on a reporting business entity; and

(d) an entity (the ***extorting entity***) makes a demand of the reporting business entity, or any other entity, in order to benefit from the incident or the impact on the reporting business entity; and

(e) the reporting business entity provides, or is aware that another entity has provided on their behalf, a payment or benefit (a ***ransomware payment***) to the extorting entity that is directly related to the demand.

(2) An entity is a ***reporting business entity*** if, at the time the ransomware payment is made:

(a) the entity:

(i) is carrying on a business in Australia with an annual turnover for the previous financial year that exceeds the turnover threshold for that year; and

(ii) is not a Commonwealth body or a State body; and

(iii) is not a responsible entity for a critical infrastructure asset; or

(b) the entity is a responsible entity for a critical infrastructure asset to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies.

(3) For the purposes of subparagraph (2)(a)(i), the ***turnover threshold*** is:

(a) if a business has been carried on for only part of the previous financial year—the amount worked out in the manner prescribed by the rules; or

(b) in any other case—the amount prescribed by, or worked out in the manner prescribed by, the rules.

Presumption

(4) For the purposes of paragraph (1)(b), an incident (other than an incident covered by paragraph 9(2)(a) or (b)) is presumed to be a cyber security incident if:

(a) the incident was probably effected, is probably being effected or could reasonably be expected to be effected, by means of a telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution (including, for example, by means of the internet); or

(b) the incident has probably impeded or impaired, or is probably impeding or impairing or could reasonably be expected to impede or impair, the ability of a computer to connect to such a service; or

(c) the incident has probably seriously prejudiced, is probably 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.

Note: Paragraphs 9(2)(a) and (b) cover incidents involving critical infrastructure assets or the activities of corporations to which paragraph 51(xx) of the Constitution applies.

(5) However, subsection (4) does not make an entity liable to a civil penalty under this Part if the incident:

(a) was not in fact effected by means of a telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution (including, for example, by means of the internet); or

(b) did not in fact impede or impair the ability of a computer to connect to such a service; or

(c) did not in fact seriously prejudice:

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

(ii) the defence of Australia; or
(iii) national security.

27 Obligation to report following a ransomware payment

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

Note: For the definition of ***designated Commonwealth body***: see section 8.

(2) The ransomware payment report must contain information relating to the following, in accordance with any requirements prescribed by the rules, that, at the time of making the report, the reporting business entity knows or is able, by reasonable search or enquiry, to find out:

(a) if the reporting business entity made the payment—the reporting business entity's contact and business details;
(b) if another entity made the payment—that entity's contact and business details;
(c) the cyber security incident, including its impact on the reporting business entity;
(d) the demand made by the extorting entity;
(e) the ransomware payment;
(f) communications with the extorting entity relating to the incident, the demand and the payment.

(3) The reporting business entity may include other information relating to the cyber security incident in the ransomware payment report.

(4) The ransomware payment report must be given:

(a) in the form approved by the Secretary (if any); and
(b) in the manner (if any) prescribed by the rules.

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

Civil penalty: 60 penalty units.

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

28 Liability

(1) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with section 27.

(2) An officer, employee or agent of an entity is not liable to an action for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1).

(3) An entity that wishes to rely on subsection (1) in relation to an action or other proceeding bears an evidential burden (within the meaning of the Regulatory Powers Act) in relation to that matter.

Division 3—Protection of information

29 Ransomware payment reports may only be used or disclosed for permitted purposes

Permitted use and disclosure

(1) A designated Commonwealth body may make a record of, use or disclose information provided in a ransomware payment report by a reporting business entity, but only for the purposes of one or more of the following:

(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;

(b) performing functions or exercising powers under this Part or Part 6 as it applies to this Part;

(c) proceedings under, or arising out of, section 137.1 or 137.2 of the *Criminal Code* (false and misleading information and documents) that relate to this Act;

(d) 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;

(e) the performance of the functions of a Commonwealth body relating to responding to, mitigating or resolving a cyber security incident;

(f) the performance of the functions of a State body relating to responding to, mitigating or resolving a cyber security incident;

(g) the performance of the functions of the National Cyber Security Coordinator under Part 4 relating to a cyber security incident;

(h) informing and advising the Minister, and other Ministers of the Commonwealth, about a cyber security incident;

(i) the performance of the functions of an intelligence agency.

Note: Certain information must not be disclosed to a State body under Parts of this Act unless a Minister of the State or Territory has consented to those Parts applying to the State body: see section 11.

Restriction on use and disclosure for civil or regulatory action

(2) However, the designated Commonwealth body 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 reporting business entity of a Commonwealth, State or Territory law other than:

(a) a contravention by the reporting business entity of this Part; or

(b) a contravention by the reporting business entity of a law that imposes a penalty or sanction for a criminal offence.

Note: See also section 32 in relation to admissibility of the information in proceedings against the reporting business entity.

Interaction with the Privacy Act 1988

(3) Subsection (1) does not authorise the designated Commonwealth body to record, use or disclose the information to the extent that it is prohibited or restricted by or under the *Privacy Act 1988*.

Information not covered by the prohibitions in this section

(4) Subsection (1) does not prohibit the recording, use or disclosure of the following information:

(a) information that has been provided to the designated Commonwealth body by, or on behalf of, the entity to the Commonwealth to comply with:

(i) a requirement in Part 2B of the *Security of Critical Infrastructure Act 2018*; or

(ii) a requirement under the *Telecommunications Act 1997*; or

(iii) a requirement under a law prescribed by the rules;

(b) information that has already been lawfully made available to the public.

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

(1) This section applies to information that:

(a) has been provided in a ransomware payment report by a reporting business entity; and

(b) has been obtained by another entity, Commonwealth body or State body under subsection 29(1) or this section; and

(c) is held by the other entity, Commonwealth body or State body.

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.

Permitted use and disclosure

(2) The other entity, Commonwealth body or State body may make a record of, use or disclose the information but only for the purposes of one or more of the following:

(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;

(b) performing functions or exercising powers under this Part or Part 6 as it applies to this Part;

(c) proceedings under, or arising out of, section 137.1 or 137.2 of the *Criminal Code* (false and misleading information and documents) that relate to this Act;

(d) 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;

(e) the performance of the functions of a Commonwealth body relating to responding to, mitigating or resolving a cyber security incident;

(f) the performance of the functions of a State body relating to responding to, mitigating or resolving a cyber security incident;

(g) the performance of the functions of the National Cyber Security Coordinator under Part 4 relating to a cyber security incident;

(h) informing and advising the Minister, and other Ministers of the Commonwealth, about a cyber security incident;

(i) the performance of the functions of an intelligence agency.

Restriction on use and disclosure for civil or regulatory action

(3) However, the other entity, Commonwealth body or State body 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 reporting business entity, of a Commonwealth, State or Territory law other than:

(a) a contravention by the reporting business entity of this Part; or

(b) a contravention by the reporting business entity of a law that imposes a penalty or sanction for a criminal offence.

Interaction with the Privacy Act 1988

(4) Subsection (2) does not authorise the other entity, Commonwealth body or State body to record, use or disclose the information to the extent that it is prohibited or restricted by or under the *Privacy Act 1988*.

Information not covered by the prohibitions in this section

(5) Subsection (2) does not prohibit:

(a) recording, use or disclosure of information referred to in subsection 29(4); or

(b) if the other entity is an individual—recording, use or disclosure of personal information about the individual; or

(c) recording, use or disclosure of the reporting business entity's own information, with the consent of the reporting business entity, by another entity, a Commonwealth body or a State body; or

(d) recording, use or disclosure of information for the purposes of carrying out a State's constitutional functions, powers or duties.

Civil penalty for contravention of this section

(6) An entity is liable to a civil penalty if:

(a) the entity contravenes subsection (2); and

(b) the entity is not a Commonwealth officer; and

(c) any of the following applies:

(i) the information is sensitive information about an individual and the individual has not consented to the record, use or disclosure of the information;

(ii) the information is confidential or commercially sensitive;

(iii) the record, use or disclosure of the information would, or could reasonably be expected to, cause damage to the security, defence or international relations of the Commonwealth.

Note 1: See the *Criminal Code* for offences for Commonwealth officers.

Note 2: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.

Civil penalty: 60 penalty units.

31 Legal professional privilege

(1) The fact that a reporting business entity provided information in a ransomware payment report does not otherwise affect a claim of legal professional privilege that anyone may make in relation to that information in any proceedings:

(a) under any Commonwealth, State or Territory law (including the common law); or

(b) before a tribunal of the Commonwealth, a State or a Territory.

(2) Despite subsection (1), this section does not apply to the following:

(a) the proceedings of a coronial inquiry or a Royal Commission in Australia;

(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.

Note: For ***federal court***, see section 2B of the *Acts Interpretation Act 1901*.

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

32 Admissibility of information in ransomware payment report against reporting business entity

(1) This section applies to information that:

(a) has been provided in a ransomware payment report by a reporting business entity; and

(b) has been obtained by a Commonwealth body or State body under section 27, subsection 29(1) or section 30; and

(c) is held by the Commonwealth body or State body.

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.

(2) That information is not admissible in evidence against the reporting business entity in any of the following proceedings:

(a) criminal proceedings for an offence against a Commonwealth, State or Territory law, other than:

(i) proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* (which deal with false or misleading information or documents) that relates to this Act; or

(ii) proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act;

(b) civil proceedings for a contravention of a civil penalty provision of a Commonwealth, State or Territory law, other than a civil penalty provision of this Part;

(c) proceedings for a breach of any other Commonwealth, State or Territory law (including the common law);

(d) proceedings before a tribunal of the Commonwealth, a State or a Territory.

(3) However, this section does not apply to the following:

(a) the proceedings of a coronial inquiry or a Royal Commission in Australia;

(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.

Note: For federal court, see section 2B of the *Acts Interpretation Act 1901*.

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

Part 4—Coordination of significant cyber security incidents

Division 1—Preliminary

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

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

(1) This section applies if:

(a) an incident has occurred, is occurring or is imminent; and

(b) the incident is a cyber security incident; and

(c) the incident has had, is having, or could reasonably be expected to have, a direct or indirect impact on an entity (the ***impacted entity***); and

(d) the impacted entity is:

(i) carrying on a business in Australia; or

(ii) a responsible entity for a critical infrastructure asset to which the *Security of Critical Infrastructure Act 2018* applies.

(2) The impacted entity, or another entity acting on behalf of the impacted entity, may provide information about the incident to the National Cyber Security Coordinator if:

(a) the incident is a significant cyber security incident; or

(b) the incident could reasonably be expected to be a significant cyber security incident.

Note 1: For information provided in relation to other kinds of cyber security incidents: see sections 36 and 39.

Note 2: This subsection constitutes an authorisation for the National Cyber Security Coordinator to collect the information (including sensitive information) for the purposes of the *Privacy Act 1988*.

(3) Information about the incident may be provided under subsection (2):

(a) at any time during the response to the incident; and

(b) on the impacted entity's own initiative or in response to a request by the National Cyber Security Coordinator.

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

Presumption

(4) For the purposes of paragraph (1)(b), an incident (other than an incident covered by paragraph 9(2)(a) or (b)) is presumed to be a cyber security incident if:

(a) the incident was probably effected, is probably being effected or could reasonably be expected to be effected, by means of a telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution (including, for example, by means of the internet); or

(b) the incident has probably impeded or impaired, or is probably impeding or impairing or could reasonably be expected to impede or impair, the ability of a computer to connect to such a service; or

(c) the incident has probably seriously prejudiced, is probably 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.

Note: Paragraphs 9(2)(a) and (b) covers incidents involving critical infrastructure assets or the activities of corporations to which paragraph 51(xx) of the Constitution applies.

(5) However, subsection (4) does not make an entity liable to a civil penalty under this Part if the incident:

(a) was not in fact effected by means of a telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution (including, for example, by means of the internet); or

(b) did not in fact impede or impair the ability of a computer to connect to such a service; or

(c) did not in fact seriously prejudice:

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

(ii) the defence of Australia; or

(iii) national security.

36 Voluntary provision of information in relation to other incidents or cyber security incidents

(1) This section applies if:

(a) an incident has occurred, is occurring or is imminent; and

(b) an entity (the ***impacted entity***) provides information to the National Cyber Security Coordinator in relation to the incident; and

(c) it is unclear at the time the information is provided whether the incident is a cyber security incident or a significant cyber security incident.

(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.

Note: This subsection constitutes an authorisation for the National Cyber Security Coordinator to collect the information (including sensitive information) for the purposes of the *Privacy Act 1988*.

37 Role of the National Cyber Security Coordinator

The role of the National Cyber Security Coordinator includes, but is not limited to, the following:

(a) to lead across the whole of Government the coordination and triaging of action in response to a significant cyber security incident;

(b) to inform and advise the Minister and the whole of Government in relation to the whole of Government response to a significant cyber security incident.

Division 3—Protection of information

38 Information provided in relation to a significant cyber security incident—use and disclosure by National Cyber Security Coordinator

Permitted use and disclosure

(1) The National Cyber Security Coordinator may make a record of, use or disclose information provided under subsection 35(2) by, or on behalf of, an entity (the ***impacted entity***) in relation to a cyber security incident but only for the purposes of one or more of the following:

(a) assisting the impacted entity, and other entities acting on behalf of the impacted entity, to respond to, mitigate or resolve the cyber security incident;

(b) a permitted cyber security purpose for a cyber security incident.

Note 1: For ***permitted cyber security purpose*** for a cyber security incident: see section 10. This includes the functions of the National Cyber Security Coordinator under this Part.

Note 2: Certain information must not be disclosed to a State body under Parts of this Act unless a Minister of the State or Territory has consented to those Parts applying to the State body: see section 11.

Restriction on use and disclosure for civil or regulatory action

(2) However, the National Cyber Security Coordinator 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 impacted entity of a Commonwealth, State or Territory law other than:

(a) a contravention by the impacted entity of this Part; or

(b) a contravention by the impacted entity of a law that imposes a penalty or sanction for a criminal offence.

Note: See also section 42 in relation to admissibility of the information in proceedings against the impacted entity.

Interaction with the Privacy Act 1988

(3) Subsection (1) does not authorise the National Cyber Security Coordinator to record, use or disclose the information to the extent that it is prohibited or restricted by or under the *Privacy Act 1988*.

Information not covered by the prohibitions in this section

(4) Subsection (1) does not prohibit the recording, use or disclosure of the following information:

(a) information that has been provided by, or on behalf of, the impacted entity to the Commonwealth about the cyber security incident to comply with:

(i) a requirement in Part 3 of this Act; or

(ii) a requirement in Part 2B of the *Security of Critical Infrastructure Act 2018*; or

(iii) a requirement under the *Telecommunications Act 1997*; or

(iv) a requirement under a law prescribed by the rules;

(b) information that has been provided voluntarily to the National Cyber Security Coordinator by, or on behalf of, the impacted entity, other than under this Part;

(c) information that has already been lawfully made available to the public.

39 Information provided in relation to other incidents—use and disclosure by National Cyber Security Coordinator

(1) This section applies if:

(a) an incident has occurred, is occurring or is imminent; and

(b) an entity (the ***impacted entity***) provides information to the National Cyber Security Coordinator in relation to the incident; and

(c) the incident either:

(i) is not a cyber security incident; or

(ii) is a cyber security incident but is not a significant cyber security incident.

Permitted use and disclosure

(2) The National Cyber Security Coordinator may make a record of, use or disclose the information provided by the impacted entity but only for the purposes of one or more of the following:

(a) directing the impacted entity to other services that may assist the entity to respond to, mitigate, or resolve the incident;

(b) if the incident is a cyber security incident—coordinating the whole of Government response to the cyber security incident where the National Cyber Security Coordinator considers such a response is necessary;

(c) if the incident is a cyber security incident—informing and advising the Minister, and other Ministers of the Commonwealth, about the cyber security incident.

Restriction on use and disclosure for civil or regulatory action

(3) However, the National Cyber Security Coordinator 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 impacted entity of a Commonwealth, State or Territory law other than:

(a) a contravention by the impacted entity of this Part; or

(b) a contravention by the impacted entity of a law that imposes a penalty or sanction for a criminal offence.

Note: See also section 42 in relation to admissibility of the information in proceedings against the impacted entity.

Interaction with the Privacy Act 1988

(4) Subsection (2) does not authorise the National Cyber Security Coordinator to record, use or disclose the information to the extent that it is prohibited or restricted by or under the *Privacy Act 1988*.

Information not covered by the prohibitions in this section

(5) Subsection (2) does not prohibit the recording, use or disclosure of the following information:

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

40 Limitations on secondary use and disclosure

(1) This section applies to information that:
  (a) has been provided by, or on behalf of, an entity (the ***impacted entity***) under subsection 35(2) or as referred to in subsection 39(1); and
  (b) has been obtained by another entity, a Commonwealth body (other than ASD) or a State body under subsection 38(1) or 39(2) or this section; and
  (c) is held by the other entity, Commonwealth body or State body.

Note 1: 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.

Note 2: For ASD, see Division 1A of Part 6 of the *Intelligence Services Act 2001*.

Permitted use and disclosure

(2) The other entity, Commonwealth body or State body may make a record of, use or disclose the information but only for the purposes of one or more of the following:

(a) assisting the impacted entity, and other entities acting on behalf of the impacted entity, to respond to, mitigate or resolve the cyber security incident;

(b) a permitted cyber security purpose for a cyber security incident.

Note: For ***permitted cyber security purpose*** for a cyber security incident: see section 10.

Restriction on use and disclosure for civil or regulatory action

(3) However, the other entity, Commonwealth body or State body 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 impacted entity of a Commonwealth, State or Territory law other than:

(a) a contravention by the impacted entity of this Part; or

(b) a contravention by the impacted entity of a law that imposes a penalty or sanction for a criminal offence.

Interaction with the Privacy Act 1988

(4) Subsection (2) does not authorise the other entity, Commonwealth body or State body to record, use or disclose the information to the extent that it is prohibited or restricted by or under the *Privacy Act 1988*.

Information not covered by the prohibitions in this section

(5) Subsection (2) does not prohibit:

(a) recording, use or disclosure of information referred to in subsection 38(4) or 39(5); or

(b) if the other entity is an individual—recording, use or disclosure of personal information about the individual; or

(c) recording, use or disclosure of the impacted entity's own information, with the consent of the impacted entity, by another entity, a Commonwealth body or a State body; or

(d) recording, use or disclosure for the purposes of carrying out a State's constitutional functions, powers or duties.

Civil penalty for contravention of this section

(6) An entity is liable to a civil penalty if:

(a) the entity contravenes subsection (2); and

(b) the entity is not a Commonwealth officer; and

(c) any of the following applies:

(i) the information is sensitive information about an individual and the individual has not consented to the record, use or disclosure of the information;

(ii) the information is confidential or commercially sensitive;

(iii) the record, use or disclosure of the information would, or could reasonably be expected to, cause damage to the security, defence or international relations of the Commonwealth.

Note 1: See the *Criminal Code* for offences for Commonwealth officers.

Note 2: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.

Civil penalty: 60 penalty units.

41 Legal professional privilege

(1) The fact that an entity provided information to the National Cyber Security Coordinator under subsection 35(2), or as referred to in subsection 39(1), does not otherwise affect a claim of legal professional privilege that anyone may make in relation to that information in any proceedings:

(a) under any Commonwealth, State or Territory law (including the common law); or

(b) before a tribunal of the Commonwealth, a State or a Territory.

(2) Despite subsection (1), this section does not apply to the following:

(a) the proceedings of a coronial inquiry or a Royal Commission in Australia;

(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.

Note: For ***federal court***, see section 2B of the *Acts Interpretation Act 1901*.

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

42 Admissibility of information voluntarily given by impacted entity

(1) This section applies to information that:

(a) has been provided by, or on behalf of, an entity (the ***impacted entity***) under subsection 35(2) or as referred to in subsection 39(1); and

(b) has been obtained by a Commonwealth body or State body under subsection 35(2), 38(1), 39(1), 39(2) or 40(2); and

(c) is held by the Commonwealth body or State body.

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.

(2) That information is not admissible in evidence against the impacted entity in any of the following proceedings:

(a) criminal proceedings for an offence against a Commonwealth, State or Territory law, other than:

(i) proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* (which deal with false or misleading information or documents) that relates to this Act; or

(ii) proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act;

(b) civil proceedings for a contravention of a civil penalty provision of a Commonwealth, State or Territory law, other than a civil penalty provision of this Part;

(c) proceedings for a breach of any other Commonwealth, State or Territory law (including the common law);

(d) proceedings before a tribunal of the Commonwealth, a State or a Territory.

(3) However, this section does not apply to the following:

(a) the proceedings of a coronial inquiry or a Royal Commission in Australia;

(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.

Note: For ***federal court***, see section 2B of the *Acts Interpretation Act 1901*.

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

43 National Cyber Security Coordinator not compellable as witness

(1) The Secretary may issue a certificate stating that:

(a) a specified person is, or has been:

(i) a person referred to in paragraph (a) of the definition of ***National Cyber Security Coordinator*** in section 8; or

(ii) a person referred to in paragraph (b) of the definition of ***National Cyber Security Coordinator*** in section 8; and

(b) the specified person is involved, or has been involved, in a specified matter in which the National Cyber Security Coordinator is performing or has performed functions or is exercising or has exercised powers under this Part.

(2) If, under subsection (1), the Secretary issues a certificate in relation to a person and a specified matter, the person:

(a) is not obliged to comply with a subpoena or similar direction of a federal court or a court of a State or Territory to attend and answer questions relating to the matter; and

(b) is not compellable to give an expert opinion in any civil or criminal proceedings in a federal court or a court of a State or Territory in relation to the matter;

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

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

Division 4—Miscellaneous

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

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

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

Part 5—Cyber Incident Review Board

Division 1—Preliminary

45 Simplified outline of this Part

The Cyber Incident Review Board is established by this Part.

The Board must cause reviews to be conducted in relation to certain cyber security incidents. The purpose of a review is to make recommendations to government and industry about actions that could be taken to prevent, detect, respond to or minimise the impact of, cyber security incidents of a similar nature in the future.

A review panel will be established for each review in accordance with the terms of reference for the review.

The Board consists of the Chair and up to 6 other standing members. The standing members are appointed by the Minister.

The Board may establish an Expert Panel. One or more members of the Expert Panel may be appointed to assist in relation to a review conducted under this Part.

This Part also deals with the appointment of the Chair, standing members and Expert Panel members, and the procedures of the Board.

Division 2—Reviews

46 Board must cause reviews to be conducted

(1) The Cyber Incident Review Board may cause a review to be conducted under this section in relation to a cyber security incident, or a series of related cyber security incidents, on written referral by:

(a) the Minister; or

(b) the National Cyber Security Coordinator; or

(c) an entity impacted by the incident or an incident in the series of incidents; or

(d) a member of the Board.

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:

(a) the incident or series of incidents have seriously prejudiced, or could reasonably be expected to seriously prejudice:

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

(ii) the defence of Australia; or

(iii) national security; or

(b) the incident or series of incidents involved novel or complex methods or technologies, an understanding of which will significantly improve Australia's preparedness, resilience, or response to cyber security incidents of a similar nature; or

(c) the incident or series of incidents are, or could reasonably be expected to be, of serious concern to the Australian people.

(4) Each review is to be conducted by a review panel that consists of:
(a) the Chair; and
(b) the standing members of the Board that are specified in the terms of reference for the review; and
(c) the members of the Expert Panel appointed to assist in the review under section 70.

The terms of reference for the review must specify one or more standing members for the review.

(5) The rules may make provision for or in relation to reviews under this Part, including for or in relation to the following:
(a) dealing with written referrals made to the Board;
(b) prioritisation of referrals for review and reviews conducted;
(c) terms of reference for reviews, including their variation;
(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 provided 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 review, publish in any way the Board considers appropriate notice of the review being discontinued.

48 Chair may request information or documents

If the Board reasonably believes that:
(a) an entity; or
(b) a Commonwealth body or a State body; or
(c) an officer or employee of a Commonwealth body or a State body;

has information or documents relevant to a review being conducted under section 46 by a review panel, the Chair may request, by notice in writing, the entity, body, officer or employee to give the

Board such information or documents as are specified in the request.

Note 1: There is no requirement to comply with the request.

Note 2: The Chair may require certain entities to give documents under section 49.

49 Chair may require certain entities to produce documents

(1) This section applies if:

(a) the Board reasonably believes that an entity involved in a cyber security incident that relates to a review being conducted under section 46 by a review panel has a document that is relevant to the review; and

(b) the Chair of the Board has requested that the entity provide the document under section 48; and

(c) the entity is not:

(i) a Commonwealth body or a State body; or

(ii) an officer or employee of a Commonwealth body or a State body.

(2) The Chair of the Board may, by notice in writing given to the entity, require the entity to:

(a) produce any such documents; or

(b) make copies of any such documents and to produce those copies;

to the Board within the period (which must not be less than 14 days), and in the manner, specified in the notice.

(3) The notice must set out the effect of the following provisions:

(a) section 50;

(b) Part 6 of this Act (Regulatory powers);

(c) sections 137.1 and 137.2 of the *Criminal Code* (false or misleading information or documents).

Compensation

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

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

(1) An entity is liable to a civil penalty if:

(a) the entity is given a notice under subsection 49(2); and

(b) the entity fails to comply with the notice.

Civil penalty: 60 penalty units.

(2) Subsection (1) does not apply in relation to the production of a document or a copy of a document if the production would, or could reasonably be expected to, prejudice one or more of the following:

(a) the security, defence or international relations of the Commonwealth;

(b) the capabilities of an intelligence agency;

(c) the prevention, detection or investigation of, or the conduct of proceedings relating to, an offence or a contravention of a civil penalty provision;

(d) the administration of justice.

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

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

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

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 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 *Privacy Act 1988*). 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

within which submissions may be made to the Board on the draft review report.

(6) Submissions must be given in the manner and form (if any) prescribed by the rules.

(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 *Privacy Act 1988* or any other Act.

52 Final review reports

(1) After a review is completed under section 46 by the review panel, the Board must prepare a report (a ***final review report***) on the review.

Note 1: The Board must redact sensitive review information from a final review report: see section 53.

Note 2: If information is redacted from a final review report, the Board must also prepare a protected review report: see section 54.

(2) In preparing the final review report, the Board must consider any submissions received under section 51 in relation to the draft review report.

(3) Subject to section 53, the final review report must set out:

(a) the findings of the review; and

(b) a summary of the information and material on which those findings are based; and

(c) any recommendations made by the Board; and

(d) if recommendations are made—the reasons for those recommendations; and

(e) if the terms of reference for the review require particular information to be included in the 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 report.

(4) The Board must not in the final review report:

(a) apportion blame in relation to a cyber security incident that was the subject of the review; or

(b) provide the means to determine the liability of any entity in relation to such a cyber security incident; or

(c) identify an individual (unless the individual has consented); or

(d) allow any adverse inference to be drawn from the fact that an entity is the subject of the review.

However, even though blame or liability may be inferred, or an adverse inference may be made, by a person other than the Board, this does not prevent the Board from including information in the final review report.

(5) This section does not otherwise limit what may be included in the final review report.

(6) The Board must publish the final review report (excluding any information required to be redacted under section 53). The report may be published in any way the Board considers appropriate.

53 Certain information must be redacted from final review reports

(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.

(2) ***Sensitive review information*** is information the disclosure of which:

(a) could prejudice the security, defence or international relations of Australia; or

(b) would prejudice relations between the Commonwealth government and the government of a State or Territory; or

(c) could reveal, or enable a person to ascertain, the existence or identity of a confidential source of information in relation to the enforcement of the criminal law; or

(d) could endanger a person's life or physical safety; or

(e) would prejudice the fair trial of any person or the impartial adjudication of a matter; or

(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

(g) would involve unreasonably disclosing information that is confidential or commercially sensitive; or

(h) would involve the disclosure of personal information about an individual without their consent.

54 Protected review reports

(1) If information must be redacted from a final review report under section 53, the Board must prepare another report (a ***protected review report***) that includes:

(a) the redacted information; and

(b) the reasons for redacting the information from the final review report.

(2) If a protected review report is prepared under this section, the Board must give the Minister, and the Prime Minister, a copy of:

(a) the final review report prepared under section 52; and

(b) a copy of the protected review report.

(3) The Minister may give a copy of the protected review report, or an 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:

(a) the performance of the functions of a Commonwealth body relating to responding to, mitigating or resolving a cyber security incident;

(b) the performance of the functions of a State body relating to responding to, mitigating or resolving a cyber security incident;

(c) informing and advising the Minister, and other Ministers of the Commonwealth, about a cyber security incident;

(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

Permitted use and disclosure

(1) The Board may make a record of, use or disclose information provided by an entity, Commonwealth body or State body under section 48, 49 or 51 but only:

(a) for the purposes of one or more of the following:

(i) performing functions or exercising powers under this Part or Part 6 as it applies to this Part;

(ii) proceedings under, or arising out of, section 137.1 or 137.2 of the *Criminal Code* (false and misleading information and documents) that relate to this Act;

(iii) proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act;

(iv) the performance of the functions of a Commonwealth body relating to responding to, mitigating or resolving a cyber security incident;

(v) the performance of the functions of a State body relating to responding to, mitigating or resolving a cyber security incident;

(vi) informing and advising the Minister, and other Ministers of the Commonwealth, about a cyber security incident;

(vii) the performance of the functions of an intelligence agency; or

(b) as otherwise authorised by a provision of this Part.

Note: Certain information must not be disclosed to a State body under Parts of this Act unless a Minister of the State or Territory has consented to those Parts applying to the State body: see section 11.

Restriction on use and disclosure for civil or regulatory action

(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:

(a) a contravention by the entity or body of this Part; or

(b) a contravention by the entity or body of a law that imposes a penalty or sanction for a criminal offence.

Note: See also section 58 in relation to admissibility of the information in proceedings.

Interaction with the Privacy Act 1988

(3) Subsection (1) 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 *Privacy Act 1988*.

Information not covered by the prohibitions in this section

(4) Subsection (1) does not prohibit the recording, use or disclosure of information that has already been lawfully made available to the public.

56 Limitations on secondary use and disclosure

(1) This section applies to information that:

(a) has been provided to the Board under section 48, 49 or 51; and

(b) has been obtained under section 54 or 55, or this section, by an entity, a Commonwealth body or a State body; and

(c) is held by the entity, Commonwealth body or State body.

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.

Permitted use and disclosure

(2) The entity, Commonwealth body or State body may make a record of, use or disclose the information but only:

(a) for the purposes of one or more of the following:

(i) performing functions or exercising powers, or assisting in the performance of functions or the exercise of powers, under this Part or Part 6 as it applies to this Part;

(ii) proceedings under, or arising out of, section 137.1 or 137.2 of the *Criminal Code* (false and misleading information and documents) that relate to this Act;

(iii) proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act;

(iv) the performance of the functions of a Commonwealth body relating to responding to, mitigating or resolving a cyber security incident;

(v) the performance of the functions of a State body relating to responding to, mitigating or resolving a cyber security incident;

(vi) informing and advising the Minister, and other Ministers of the Commonwealth, about a cyber security incident;

(vii) the performance of the functions of an intelligence agency; or

(b) as otherwise authorised by a provision of this Part.

Restriction on use and disclosure for civil or regulatory action

(3) However, the entity, Commonwealth body or State body 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 that originally provided the information under section 48, 49 or 51, of a Commonwealth, State or Territory law other than:

(a) a contravention by the entity or body of this Part; or

(b) a contravention by the entity or body of a law that imposes a penalty or sanction for a criminal offence.

Note: See also section 58 in relation to admissibility of the information in proceedings.

Interaction with the Privacy Act 1988

(4) Subsection (2) does not authorise the entity, Commonwealth body or State body to record, use or disclose the information to the extent that it is prohibited or restricted by or under the *Privacy Act 1988*.

Information not covered by the prohibitions in this section

(5) Subsection (2) does not prohibit:

(a) recording, use or disclosure of information that has already been lawfully made available to the public (for example, in the publication of the final review report); or

(b) if the entity is an individual—recording, use or disclosure of personal information about the individual; or

(c) if the entity or body is the entity or body that originally provided the information under section 48, 49 or 51—the entity's or body's own information; or

(d) recording, use or disclosure of that entity's or body's own 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 of carrying out a State's constitutional functions, powers or duties.

Civil penalty for contravention of this section

(6) An entity is liable to a civil penalty if:

(a) the entity contravenes subsection (2); and

(b) the entity is not a Commonwealth officer; and

(c) any of the following applies:

(i) the information is sensitive information about an individual and the individual has not consented to the record, use or disclosure of the information;

(ii) the information is confidential or commercially sensitive;

(iii) the record, use or disclosure of the information would, or could reasonably be expected to, cause damage to the security, defence or international relations of the Commonwealth.

Note 1: See the *Criminal Code* for offences for Commonwealth officers.

Note 2: This Act does not make the Crown (other than an authority of the Crown) liable to a civil penalty.

Civil penalty: 60 penalty units.

57 Legal professional privilege

(1) The fact that an entity provided information to the Board under section 48, 49 or 51 does not otherwise affect a claim of legal professional privilege that anyone may make in relation to that information in any proceedings:

(a) under any Commonwealth, State or Territory law (including the common law); or

(b) before a tribunal of the Commonwealth, a State or a Territory.

(2) Despite subsection (1), this section does not apply to the following:

(a) the proceedings of a coronial inquiry or a Royal Commission in Australia;

(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.

Note: For ***federal court***, see section 2B of the *Acts Interpretation Act 1901*.

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

58 Admissibility of information given by an entity that has been requested or required by the Board

(1) This section applies to information that:

(a) has been provided by an entity to the Board under section 48, 49 or 51; and

(b) has been obtained under section 48, 49, 51, 54, 55 or 56 by a Commonwealth body or a State body; and

(c) is held by the Commonwealth body or State body.

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.

(2) The information is not admissible in evidence against the entity in any of the following proceedings:

(a) criminal proceedings for an offence under a Commonwealth law, other than:

(i) proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* (which deal with false or misleading information or documents) that relates to this Act; or

(ii) proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act;

(b) civil proceedings for a contravention of a civil penalty provision of a Commonwealth law, other than a civil penalty provision of this Part;

(c) proceedings for a breach of any other Commonwealth, State or Territory law (including the common law);

(d) proceedings before a tribunal of the Commonwealth, a State or a Territory.

(4) This section does not apply to the following:

(a) the proceedings of a coronial inquiry or a Royal Commission in Australia;

(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.

Note: For ***federal court***, see section 2B of the *Acts Interpretation Act 1901*.

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

59 Disclosure of draft review reports prohibited

(1) An entity is liable to a civil penalty if:

(a) the entity receives a draft review report under section 51; and

(b) the entity makes a record of, discloses or otherwise uses any information in the draft review report.

Civil penalty: 60 penalty units.

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

(a) for the purpose of preparing a submission to the Board in accordance with section 51; or

(b) if the entity is the entity that originally provided the information under section 48 or 49—of the entity's own information; or

(c) with the consent of the Chair of the Board; or

(d) after the information has already been lawfully made available to the public (for example, in the publication of the final review report);

(e) for the purposes of carrying out a State's constitutional functions, powers or duties.

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

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

Division 4—Establishment, functions and powers of the Board

60 Cyber Incident Review Board

(1) The Cyber Incident Review Board is established by this section.

(2) For the purposes of paragraph (a) of the definition of ***Department of State*** in section 8 of the *Public Governance, Performance and Accountability Act 2013*, the Cyber Incident Review Board is prescribed in relation to the Department.

Note: Subject to subsection (2), this means that the chair and members of the Board are officials of the Department for the purposes of the *Public Governance, Performance and Accountability Act 2013*.

61 Constitution of the Board

The Board consists of the following members:

(a) a Chair;

(b) at least 2, and not more than 6, other standing members.

62 Functions of the Board

(1) The functions of the Board are:

(a) to cause reviews to be conducted by review panels in relation to cyber security incidents, or series of related cyber security incidents, to:

(i) identify factors that contributed to the incident or series of incidents; and

(ii) make recommendations to government and industry about actions that could be taken to prevent, detect, respond to or minimise the impact of, incidents of a similar nature in the future; and

(iii) report publicly on the review; and

(b) any other functions conferred on the Board by this Act or the rules.

Note: See section 46 in relation to the circumstances in which a cyber security incident may be reviewed.

(2) It is not a function of the Board to:

(a) apportion blame in relation to a cyber security incident; or

(b) provide the means to determine the liability of any entity in relation to a cyber security incident; or

(c) allow any adverse inference to be drawn from the fact that an entity is the subject of a review.

However, even though blame or liability may be inferred, or an adverse inference may be made, by a person other than the Board, this does not prevent the Board from carrying out its functions.

(3) The Board has power to do all things necessary or convenient to be done for or in connection with the performance of the Board's functions.

(4) The Board must not perform a function or exercise a power under this Part at a particular time if the performance of the function or the exercise of the power at that time would prejudice the investigation of, or the conduct of proceedings relating to, an offence or a contravention of a civil penalty provision under a law of the Commonwealth or of a State or Territory.

(5) The rules may prescribe the circumstances in which cyber security incidents are a series of related incidents for the purposes of this section.

Note: For example, the rules may prescribe that cyber security incidents are a series of related incidents if the incidents involve a common type of impacted system or a common attack method.

63 Independence

Subject to this Act and to other laws of the Commonwealth, the Cyber Incident Review Board:

(a) has complete discretion in the performance of the Board's functions and the exercise of the Board's powers; and

(b) is not subject to direction by any person in relation to the performance or exercise of those functions or powers.

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

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

64 Appointment of Chair

(1) The Chair of the Board is to be appointed by the Minister by written instrument.

Note: The Chair may be reappointed: see section 33AA of the *Acts Interpretation Act 1901*.

(2) The Chair may be appointed on a full-time or part-time basis.

(3) The Chair holds office for the period specified in the instrument of appointment. The period must not exceed 4 years.

(4) The rules may make provision for or in relation to the appointment of the Chair, including in relation to eligibility for appointment.

65 Remuneration of the Chair

(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.

(2) The Chair is to be paid the allowances that are prescribed by the rules.

(3) This section has effect subject to the *Remuneration Tribunal Act 1973*.

66 Appointment of standing members of the Board

(1) A standing member of the Board is to be appointed by the Minister by written instrument.

Note: A member may be reappointed: see section 33AA of the *Acts Interpretation Act 1901*.

(2) A standing member of the Board may be appointed on a full-time or part-time basis.

(3) A standing member of the Board holds office for the period specified in the instrument of appointment. The period must not exceed 4 years.

(4) The rules may make provision for or in relation to the appointment of standing members of the Board, including in relation to eligibility for appointment.

67 Remuneration of standing members of the Board

(1) A standing member 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, a standing member of the Board is to be paid the remuneration that is prescribed by the rules.

(2) A standing member of the Board is to be paid the allowances that are prescribed by the rules.

(3) This section has effect subject to the *Remuneration Tribunal Act 1973*.

68 Acting Chair

The Minister may, by written instrument, appoint a standing member of the Board to act as the Chair:

(a) during a vacancy in the office of Chair (whether or not an appointment has previously been made to the office); or

(b) during any period, or during all periods, when the Chair:

(i) is absent from duty or from Australia; or

(ii) is, for any reason, unable to perform the duties of the office.

Note: For rules that apply to acting appointments, see section 33A of the *Acts Interpretation Act 1901*.

69 Terms and conditions etc. for standing members

(1) The rules may make provision for or in relation to the Board, including for or in relation to the following:

(a) membership of the Board (subject to section 61);

(b) terms of appointment of the Chair and standing members;

(c) acting appointments;

(d) resignation of the Chair and standing members;

(e) disclosure of interests by the Chair and standing members;

(f) termination of appointment of the Chair and standing members;

(g) leave of absence of the Chair and standing members.

(2) The Chair and a standing member of the Board holds office on the terms and conditions (if any) that are determined by the Minister in relation to matters not covered by this Act or the rules.

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 *Acts Interpretation Act 1901*.

(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 *Remuneration Tribunal Act 1973*.

(5) The rules may make provision for or in relation to the Expert Panel, including for or in relation to the following:

(a) membership of the Expert Panel;
(b) appointment of members to the Expert Panel;
(c) appointments of its members to 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 Arrangements relating to staff of the Department

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

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

73 Board procedures

(1) Subject to this Act and the rules, the Board may:
  (a) operate in the way it determines; and
  (b) regulate proceedings at its meetings as it considers appropriate.

(2) The rules may make provision for or in relation to the operation and procedures of the Board.

74 Liability

Responding to notices to produce

(1) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with section 49 (Chair may obtain documents from certain entities).

(2) An officer, employee or agent of an entity is not liable to an action for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1).

The Board etc.

(3) A person who is or has been:
  (a) the Chair; or
  (b) a standing member of the Board; or
  (c) a member of the Expert Panel; or
  (d) a member of the staff assisting the Board (as mentioned in section 71); or
  (e) a consultant assisting the Board (as mentioned in section 72); or
  (f) a witness appearing in a review;

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.

Evidential burden

(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.

75 Certification of involvement in review

(1) The Chair may issue a certificate stating that a specified person who is, or has been:

(a) a standing member of the Board; or

(b) a member of the Expert Panel; or

(c) a member of the staff assisting the Board (as mentioned in section 71); or

(d) a consultant assisting the Board (as mentioned in section 72); or

(e) a witness appearing in a review;

is involved, or has been involved, in a review under this Part into a specified matter.

(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 a review under this Part into a specified matter.

(3) If, under subsection (1) or (2), a certificate is issued in relation to a person and a specified matter, the person:

(a) is not obliged to comply with a subpoena or similar direction of a federal court or a court of a State or Territory to attend and answer questions relating to the matter; and

(b) is not compellable to give an expert opinion in any civil or 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

The annual report prepared by the Secretary and given to the Minister under section 46 of the *Public Governance, Performance and Accountability Act 2013* for a reporting period must also include the following:

(a) the number of each of the following during the period:
  (i) reviews commenced;
  (ii) reviews completed;
  (iii) reviews discontinued;
(b) a brief description of each of those reviews;
(c) the status of any reviews not yet completed at the end of the period;
(d) the reasons for discontinuing any reviews during the period;
(e) the number of times the Minister refused to approve the terms of reference for a review during the period;
(f) the number of members of the Expert Panel during the period;
(g) the number of Expert Panel members appointed to a review panel during the period;
(h) the number of times appointment of a member of the Board was terminated during the period.

77 Rules may prescribe reporting requirements etc.

The rules may prescribe requirements with which the Board must comply relating to:

(a) the communication of information to the public; and
(b) reporting to the Minister;

about the work of the Board.

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 Part 6 of the *Intelligence Services Act 2001*, is subject to:

(a) monitoring under Part 2 of the Regulatory Powers Act; and

(b) investigation under Part 3 of the Regulatory Powers Act.

Sections 15 and 16 of this Act (regarding security standards) are also subject to monitoring under Part 2 of the Regulatory Powers Act.

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

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

Undertakings to comply with such civil penalty provisions, and sections 15 and 16 (regarding security standards), may be accepted and enforced under Part 6 of the Regulatory Powers Act.

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

Division 2—Civil penalty provisions, enforceable undertakings and injunctions

79 Civil penalty provisions, enforceable undertakings and injunctions

Enforceable provisions

(1) Each civil penalty provision of this Act, and each civil penalty provision of Division 1A of Part 6 of the *Intelligence Services Act 2001*, is enforceable:

(a) under Part 4 of the Regulatory Powers Act (civil penalty provisions); and

(b) Part 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 following provisions are enforceable under Part 6 (enforceable undertakings) of the Regulatory Powers Act:

(a) each civil penalty provision of this Act, and each civil penalty provision of Division 1A of Part 6 of the *Intelligence Services Act 2001*;

(b) sections 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.

Authorised applicant

(3) For the purposes of Parts 4 and 7 of the Regulatory Powers Act, each of the following persons is an authorised applicant in relation to the civil penalty provisions mentioned in subsection (1):

(a) the Secretary;

(b) a person who is appointed under subsection (4).

(4) For the purposes of paragraph (3)(b), the Secretary may, by writing, appoint a person who:

(a) is the chief executive officer (however described) of a designated Commonwealth body; or

(b) is an SES employee, or an acting SES employee, in:

(i) the Department; or

(ii) a designated Commonwealth body; or

(c) holds, or is acting in, a position in a designated Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant for the purposes of Part 4 of the Regulatory Powers Act.

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

Authorised person

(5) For the purposes of Part 6 of the Regulatory Powers Act, as that Part applies in relation to a provision mentioned in subsection (2), each of the following persons is an authorised person:

(a) the Secretary;

(b) a person who is appointed under subsection (6).

(6) For the purposes of paragraph (5)(b), the Secretary may, by writing, appoint a person who is an SES employee, or an acting SES employee in:

(a) the Department; or

(b) a designated Commonwealth body.

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

Relevant court

(7) For the purposes of Parts 4, 6 and 7 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the provisions mentioned in subsections (1) and (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 the matter.

Liability of Crown

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

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

Division 3—Monitoring and investigation powers

80 Monitoring powers

Provisions subject to monitoring

(1) The following provisions are subject to monitoring under Part 2 of the Regulatory Powers Act:

(a) each civil penalty provision of this Act;

(b) each civil penalty provision of Division 1A of Part 6 of the *Intelligence Services Act 2001*;

(c) sections 15 and 16 of this Act.

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

Information subject to monitoring

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

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

Authorised applicant

(3) For the purposes of Part 2 of the Regulatory Powers Act, a person who is appointed under subsection (4) is an authorised applicant in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

(4) The Secretary may, by writing, appoint a person who:

(a) is an SES employee, or an acting SES employee, in:

(i) the Department; or

(ii) a designated Commonwealth body; or

(b) holds, or is acting in, a position in a designated Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

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

Authorised person

(5) For the purposes of Part 2 of the Regulatory Powers Act, a person who is appointed under subsection (6) is an authorised person in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

(6) The Secretary may, by writing, appoint a person who is:

(a) an APS employee in:

(i) the Department; or

(ii) a designated Commonwealth body; or

(b) an officer or employee of a designated Commonwealth body;

to be an authorised person in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

Issuing officer

(7) For the purposes of Part 2 of the Regulatory Powers Act, a magistrate is an issuing officer in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

Relevant chief executive

(8) For the purposes of Part 2 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to the provisions mentioned in subsection (1) and information mentioned in subsection (2).

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 Investigation powers

Provisions subject to investigation

(1) Each civil penalty provision of this Act, and each civil penalty provision of Division 1A of Part 6 of the *Intelligence Services Act 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:

(a) is an SES employee, or an acting SES employee, in:

(i) the Department; or

(ii) a designated Commonwealth body; or

(b) holds, or is acting in, a position in a designated Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee;

to be an authorised applicant in relation to evidential material that relates to a provision mentioned in subsection (1).

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

Authorised person

(4) For the purposes of Part 3 of the Regulatory Powers Act, a person who is appointed under subsection (5) is an authorised person in relation to evidential material that relates to a provision mentioned in subsection (1).

(5) The Secretary may, by writing, appoint a person who is:

(a) an APS employee in:

(i) the Department; or

(ii) a designated Commonwealth body; or

(b) an officer or employee of a designated Commonwealth body;

to be an authorised person in relation to evidential material that relates to a provision mentioned in subsection (1).

Issuing officer

(6) For the purposes of Part 3 of the Regulatory Powers Act, a magistrate is an issuing officer in relation to evidential material that relates to a provision mentioned in subsection (1).

Relevant chief executive

(7) For the purposes of Part 3 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to evidential material that relates to a provision mentioned in subsection (1).

Relevant court

(8) For the purposes of Part 3 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to evidential material that relates to a provision mentioned in subsection (1):

(a) the Federal Court of Australia;

(b) the Federal Circuit and Family Court of Australia (Division 2);

(c) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

Division 4—Infringement notices

82 Infringement notices

Provisions subject to an infringement notice

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

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

Infringement officer

(2) For the purposes of Part 5 of the Regulatory Powers Act, a person authorised under subsection (3) is an infringement officer in relation to the civil penalty provisions mentioned in subsection (1).

(3) The Secretary may, by writing, authorise a person who:

(a) is an SES employee, or an acting SES employee, in:

(i) the Department; or

(ii) a designated Commonwealth body; or

(b) holds, or is acting in, a position in a designated Commonwealth body that is equivalent to, or higher than, a position occupied by an SES employee;

to be an infringement officer in relation to the civil penalty provisions mentioned in subsection (1).

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

Relevant chief executive

(4) For the purposes of Part 5 of the Regulatory Powers Act, the Secretary is the relevant chief executive in relation to the civil penalty provisions mentioned in subsection (1).

(5) The relevant chief executive may, in writing, delegate any or all of the relevant chief executive's powers and functions under Part 5 of

the Regulatory Powers Act to a person who is an SES employee or an acting SES employee in:

(a) the Department; or

(b) a designated Commonwealth body.

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

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

Liability of Crown

(7) Part 5 of the Regulatory Powers Act, as that Part applies in relation to the civil penalty provisions mentioned in subsection (1), does not make the Crown liable to be given an infringement notice.

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

Division 5—Other matters

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.

Part 7—Miscellaneous

84 Simplified outline of this Part

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.

How non-legal persons contravene this Act

(3) A provision of this Act (including a civil penalty provision) that is purportedly contravened by an entity that is not a legal person is instead contravened by each accountable person for the entity who:

(a) did the relevant act or made the relevant omission; or

(b) aided, abetted, counselled or procured the relevant act or omission; or

(c) was in any way knowingly concerned in, or party to, the relevant act or omission.

*Meaning of **accountable person***

(4) For the purposes of this section, a person is an ***accountable person*** for an entity at a particular time if:

(a) in the case of a partnership in which one or more of the partners is an individual—the individual is a partner in the partnership at that time; or

(b) in the case of a partnership in which one or more of the partners is a body corporate—the person is a director of the body corporate at that time; or

(c) in the case of a trust in which the trustee, or one or more of the trustees, is an individual—the individual is a trustee of the trust at that time; or

(d) in the case of a trust in which the trustee, or one or more of the trustees, is a body corporate—the person is a director of the body corporate at that time; or

(e) in the case of an unincorporated association—the person is a member of the governing body of the unincorporated association at that time.

86 Delegation by Secretary

(1) The Secretary may, in writing, delegate all or any of the Secretary's functions or powers under section 17, 18, 19, 21 or 23 to an SES employee, or acting SES employee, in the Department.

Note 1: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.

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

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

87 Rules

(1) The Minister may, by legislative instrument, make rules prescribing matters:

(a) required or permitted by this Act to be prescribed by the rules; or

(b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) To avoid doubt, the rules may not do the following:

(a) create an offence or civil penalty;

(b) provide powers of:

(i) arrest or detention; or

(ii) entry, search or seizure;

(c) impose a tax;

(d) set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Act;

(e) directly amend the text of this Act.

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

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

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

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

(b) consider any submissions received within the period mentioned in subparagraph (a)(ii).

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

88 Review of this Act

The Parliamentary Joint Committee on Intelligence and Security may:

(a) review the operation, effectiveness and implications of this Act; and

(b) report the Committee's comments and recommendations to each House of the Parliament;

so long as the Committee begins the review as soon as practicable after 1 December 2027.