Transport Security Amendment (Security of Australia's Transport Sector) Act 2025

No. 22, 2025

An Act to amend legislation relating to the security of aviation and maritime transport and offshore facilities, and for related purposes

Note: An electronic version of this Act is available on the Federal Register of Legislation (https://www.legislation.gov.au/)

Contents

Transport Security Amendment (Security of Australia's Transport Sector) Act 2025

No. 22, 2025

An Act to amend legislation relating to the security of aviation and maritime transport and offshore facilities, and for related purposes

[*Assented to 27 March 2025*]

The Parliament of Australia enacts:

1 Short title

This Act is the *Transport Security Amendment (Security of Australia's Transport Sector) Act 2025*.

2 Commencement

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

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	27 March 2025
2. Schedule 1	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. Schedule 2	Immediately after the commencement of the provisions covered by table item 2.	
4. Schedule 3	The day after this Act receives the Royal Assent.	28 March 2025

Note: This table relates only to the provisions of this Act as originally enacted.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

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

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—Amendments commencing day to be fixed by Proclamation

Part 1—Unlawful interference

Aviation Transport Security Act 2004

1 Section 9

Insert:

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

access to computer data means:

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

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

(i) any other location in the computer; or

(ii) another computer; or

(iii) a data storage device; or

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

(i) a computer; or

(ii) another data storage device.

asset includes:

(a) a system; and

(b) a network; and

(c) a facility; and

(d) a computer; and

(e) a computer device; and

(f) a computer program; and

(g) computer data; and

(h) premises; and

(i) any other thing.

aviation asset means an asset that:

(a) is used in connection with the operation of an aviation industry participant; and

(b) is owned or operated by an aviation industry participant.

computer means all or part of:

(a) one or more computers; or

(b) one or more computer systems; or

(c) one or more computer networks; or

(d) any combination of the above.

computer data means data held in:

(a) a computer; or

(b) a data storage device.

cyber security incident has the meaning given by section 9B.

data includes information in any form.

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

impairment of electronic communication to or from a computer includes:

(a) the prevention of any such communication; and

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

modification:

(a) in respect of computer data—means:

(i) the alteration or removal of the data; or

(ii) an addition to the data; or

(b) in respect of a computer program—means:

(i) the alteration or removal of the program; or

(ii) an addition to the program.

relevant impact has the meaning given by section 9D.

significant impact has the meaning given by section 9E.

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

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

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

unauthorised access, modification or impairment has the meaning given by section 9C.

2 After Division 4 of Part 1

Insert:

Division 4A—Cyber security incidents

9B Meaning of *cyber security incident*

A ***cyber security incident*** is one or more acts, events or circumstances involving any of the following:

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

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

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

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

9C Meaning of *unauthorised access, modification or impairment*

(1) For the purposes of this Act:
  (a) access to:

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

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

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

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

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

Note: For example, a person who is an employee or agent of an aviation industry participant is not entitled to cause access, modification or impairment of a kind mentioned in this subsection if causing such access, modification or impairment would exceed the person's authority as such an employee or agent.

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

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

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

9D Meaning of *relevant impact*

Each of the following is a ***relevant impact*** of a cyber security incident on an aviation asset:

(a) the impact (whether direct or indirect) of the incident on the availability of the asset;

(b) the impact (whether direct or indirect) of the incident on the integrity of the asset;

(c) the impact (whether direct or indirect) of the incident on the reliability of the asset;

(d) the impact (whether direct or indirect) of the incident on the confidentiality of:

(i) information about the asset; or

(ii) if information is stored in the asset—the information; or

(iii) if the asset is computer data—the computer data.

9E Meaning of *significant impact*

An impact (whether direct or indirect) of a cyber security incident on the availability of an aviation asset is a ***significant impact*** if, and only if:

(a) both:

(i) the asset is used in connection with the provision of essential goods or services; and

(ii) the incident has materially disrupted the availability of those essential goods or services; or

(b) any of the circumstances specified in the regulations exist in relation to the incident.

3 At the end of section 10

Add:

(3) A cyber security incident is an ***unlawful interference with aviation*** if the cyber security incident has had, is having, or is likely to have:

(a) a relevant impact on an aviation asset; or

(b) a significant impact on the availability of an aviation asset.

4 Paragraph 100(1)(a)

After "aviation security incident", insert "(other than a cyber security incident)".

5 At the end of section 100

Add:

Cyber security incidents

(4) An aviation industry participant who is an airport operator commits an offence if:

(a) the participant becomes aware of an aviation security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of an aviation asset; and

(b) the participant fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 12 hours, after the participant becomes so aware.

Penalty: 300 penalty units.

(5) An aviation industry participant who is an airport operator commits an offence if:

(a) the participant becomes aware of an aviation security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on an aviation asset; and

(b) the participant fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 72 hours, after the participant becomes so aware.

Penalty: 300 penalty units.

(6) Subsections (4) and (5) do not apply in relation to a report that must be made to a particular person or body if:

(a) the participant believes, on reasonable grounds, that the person or body is already aware of the incident; or

(b) the participant has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(7) Subsections (4) and (5) are offences of strict liability.

6 Paragraph 101(1)(a)

After "aviation security incident", insert "(other than a cyber security incident)".

7 At the end of section 101

Add:

Cyber security incidents

(4) An aviation industry participant who is an aircraft operator commits an offence if:

(a) the participant becomes aware of an aviation security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of an aviation asset; and

(b) the participant fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 12 hours, after the participant becomes so aware.

Penalty: 300 penalty units.

(5) An aviation industry participant who is an aircraft operator commits an offence if:

(a) the participant becomes aware of an aviation security incident that:

(i) is a cyber security incident; and
(ii) has had, is having, or is likely to have a relevant impact on an aviation asset; and

(b) the participant fails to report the incident to:
(i) the Secretary; and
(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 72 hours, after the participant becomes so aware.

Penalty: 300 penalty units.

(6) Subsections (4) and (5) do not apply in relation to a report that must be made to a particular person or body if:
(a) the participant believes, on reasonable grounds, that the person or body is already aware of the incident; or
(b) the participant has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(7) Subsections (4) and (5) are offences of strict liability.

8 Paragraph 102(1)(a)

After "aviation security incident", insert "(other than a cyber security incident)".

9 After subsection 102(3)

Insert:

Cyber security incidents

(3A) A person with incident reporting responsibilities commits an offence if:
(a) the person becomes aware of an aviation security incident that:
(i) is a cyber security incident; and
(ii) has had, is having, or is likely to have a significant impact on the availability of an aviation asset; and

(b) the person fails to report the incident to:
(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 12 hours, after the person becomes so aware.

Penalty:

(a) for a person with incident reporting responsibilities who is an aviation industry participant, other than an accredited air cargo agent—100 penalty units; and

(b) for any other person with incident reporting responsibilities—50 penalty units.

(3B) A person with incident reporting responsibilities commits an offence if:

(a) the person becomes aware of an aviation security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on an aviation asset; and

(b) the person fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 72 hours, after the person becomes so aware.

Penalty:

(a) for a person with incident reporting responsibilities who is an aviation industry participant, other than an accredited air cargo agent—100 penalty units; and

(b) for any other person with incident reporting responsibilities—50 penalty units.

(3C) Subsections (3A) and (3B) do not apply in relation to a report that must be made to a particular person or body (the ***person or body to be notified***) if:

(a) the person with incident reporting responsibilities believes, on reasonable grounds, that the person or body to be notified is already aware of the incident; or

(b) the person with incident reporting responsibilities has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(3D) Subsections (3A) and (3B) are offences of strict liability.

10 Before subsection 102(4)

Insert:

Persons with incident reporting responsibilities

11 Paragraph 103(1)(a)

After "aviation security incident", insert "(other than a cyber security incident)".

12 At the end of section 103

Add:

Cyber security incidents

(4) An employee of an aviation industry participant commits an offence if:

(a) the employee becomes aware of an aviation security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of an aviation asset; and

(b) the employee fails to report the incident to the aviation industry participant as soon as possible, and in any event within 12 hours, after the employee becomes so aware.

Penalty: 50 penalty units.

(5) An employee of an aviation industry participant commits an offence if:

(a) the employee becomes aware of an aviation security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on an aviation asset; and

(b) the employee fails to report the incident to the aviation industry participant as soon as possible, and in any event within 72 hours, after the employee becomes so aware.

Penalty: 50 penalty units.

(6) Subsections (4) and (5) do not apply if the employee has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(7) Subsections (4) and (5) are offences of strict liability.

13 Subsection 104(1)

After "aviation security incidents", insert "(other than cyber security incidents)".

14 Subsection 105(1)

After "aviation security incidents", insert "(other than cyber security incidents)".

15 Subsection 106(1)

After "aviation security incidents", insert "(other than cyber security incidents)".

Maritime Transport and Offshore Facilities Security Act 2003

16 Paragraph 6(2)(b)

After "172(1)", insert ", (4) or (5)".

17 Paragraph 6(2)(g)

After "175(1)", insert ", (3A) or (3B)".

18 Paragraph 6(2)(h)

After "176(1)", insert ", (4) or (5)".

19 Section 10

Insert:

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

access to computer data means:

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

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

(i) any other location in the computer; or

(ii) another computer; or

(iii) a data storage device; or

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

(i) a computer; or

(ii) another data storage device.

asset includes:

(a) a system; and

(b) a network; and

(c) a facility; and

(d) a computer; and

(e) a computer device; and

(f) a computer program; and

(g) computer data; and

(h) premises; and

(i) any other thing.

computer means all or part of:

(a) one or more computers; or

(b) one or more computer systems; or

(c) one or more computer networks; or

(d) any combination of the above.

computer data means data held in:

(a) a computer; or

(b) a data storage device.

cyber security incident has the meaning given by 10B.

data includes information in any form.

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

impairment of electronic communication to or from a computer includes:

(a) the prevention of any such communication; and

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

maritime asset means an asset that:

(a) is used in connection with the operation of a maritime industry participant; and

(b) is owned or operated by a maritime industry participant.

20 Section 10 (definition of *maritime transport or offshore facility security incident*)

Omit "subsections 170(1) and (2)", substitute "section 170".

21 Section 10

Insert:

modification:

(a) in respect of computer data—means:

(i) the alteration or removal of the data; or

(ii) an addition to the data; or

(b) in respect of a computer program—means:

(i) the alteration or removal of the program; or

(ii) an addition to the program.

relevant impact has the meaning given by section 10D.

significant impact has the meaning given by section 10E.

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

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

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

unauthorised access, modification or impairment has the meaning given by section 10C.

22 After Division 4 of Part 1

Insert:

Division 4A—Cyber security incidents

10B Meaning of *cyber security incident*

A ***cyber security incident*** is one or more acts, events or circumstances involving any of the following:

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

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

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

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

10C Meaning of *unauthorised access, modification or impairment*

(1) For the purposes of this Act:

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

(b) modification of:
(i) computer data; or
(ii) a computer program; or
(c) the impairment of electronic communication to or from a computer; or
(d) the impairment of the availability, reliability, security or operation of:
(i) a computer; or
(ii) computer data; or
(iii) a computer program;

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

Note: For example, a person who is an employee or agent of a maritime industry participant is not entitled to cause access, modification or impairment of a kind mentioned in this subsection if causing such access, modification or impairment would exceed the person's authority as such an employee or agent.

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

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

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

10D Meaning of *relevant impact*

Each of the following is a ***relevant impact*** of a cyber security incident on a maritime asset:

(a) the impact (whether direct or indirect) of the incident on the availability of the asset;

(b) the impact (whether direct or indirect) of the incident on the integrity of the asset;

(c) the impact (whether direct or indirect) of the incident on the reliability of the asset;

(d) the impact (whether direct or indirect) of the incident on the confidentiality of:

(i) information about the asset; or

(ii) if information is stored in the asset—the information; or

(iii) if the asset is computer data—the computer data.

10E Meaning of *significant impact*

An impact (whether direct or indirect) of a cyber security incident on the availability of a maritime asset is a ***significant impact*** if, and only if:

(a) both:

(i) the asset is used in connection with the provision of essential goods or services; and

(ii) the incident has materially disrupted the availability of those essential goods or services; or

(b) any of the circumstances specified in the regulations exist in relation to the incident.

23 Subsection 11(1)

After "following done", insert ", or attempted to be done,".

24 Paragraph 11(1)(h)

After "false", insert "or misleading".

25 At the end of section 11

Add:

(3) A cyber security incident is an ***unlawful interference with maritime transport or offshore facilities*** if the cyber security incident has had, is having, or is likely to have:

(a) a relevant impact on a maritime asset; or

(b) a significant impact on the availability of a maritime asset.

26 Subsections 170(1) and (2)

Repeal the subsections, substitute:

Each of the following is a ***maritime transport or offshore facility security incident***:

(a) a threat of unlawful interference with maritime transport or offshore facilities;

(b) an unlawful interference with maritime transport or offshore facilities.

27 Paragraph 171(1)(a)

After "maritime transport or offshore facility security incident", insert "(other than a cyber security incident)".

28 At the end of section 171

Add:

Cyber security incidents

(4) A port operator commits an offence if:

(a) the port operator becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of a maritime asset; and

(b) the port operator fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 12 hours, after the port operator becomes so aware.

Penalty: 200 penalty units.

(5) A port operator commits an offence if:

(a) the port operator becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on a maritime asset; and

(b) the port operator fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 72 hours, after the port operator becomes so aware.

Penalty: 200 penalty units.

(6) Subsections (4) and (5) do not apply in relation to a report that must be made to a particular person or body if:

(a) the port operator believes, on reasonable grounds, that the person or body is already aware of the incident; or

(b) the port operator has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(7) Subsections (4) and (5) are offences of strict liability.

29 Paragraph 172(1)(a)

After "maritime transport or offshore facility security incident", insert "(other than a cyber security incident)".

30 At the end of section 172

Add:

Cyber security incidents

(4) The master of a security regulated ship or a ship regulated as an offshore facility commits an offence if:

(a) the master becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of a maritime asset; and

(b) the master fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 12 hours, after the master becomes so aware.

Penalty: 200 penalty units.

(5) The master of a security regulated ship or a ship regulated as an offshore facility commits an offence if:

(a) the master becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on a maritime asset; and

(b) the master fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 72 hours, after the master becomes so aware.

Penalty: 200 penalty units.

(6) Subsections (4) and (5) do not apply in relation to a report that must be made to a particular person or body if:

(a) the master believes, on reasonable grounds, that the person or body is already aware of the incident; or

(b) the master has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(7) Subsections (4) and (5) are offences of strict liability.

31 Paragraph 173(1)(a)

After "maritime transport or offshore facility security incident", insert "(other than a cyber security incident)".

32 At the end of section 173

Add:

Cyber security incidents

(4) A ship operator for a security regulated ship commits an offence if:

(a) the ship operator becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of a maritime asset; and

(b) the ship operator fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 12 hours, after the ship operator becomes so aware.

Penalty: 200 penalty units.

(5) A ship operator for a security regulated ship commits an offence if:

(a) the ship operator becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on a maritime asset; and

(b) the ship operator fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 72 hours, after the ship operator becomes so aware.

Penalty: 200 penalty units.

(6) Subsections (4) and (5) do not apply in relation to a report that must be made to a particular person or body if:

(a) the ship operator believes, on reasonable grounds, that the person or body is already aware of the incident; or

(b) the ship operator has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(7) Subsections (4) and (5) are offences of strict liability.

33 Paragraph 174(1)(a)

After "maritime transport or offshore facility security incident", insert "(other than a cyber security incident)".

34 At the end of section 174

Add:

Cyber security incidents

(4) A port facility operator commits an offence if:

(a) the port facility operator becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of a maritime asset; and

(b) the port facility operator fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 12 hours, after the port facility operator becomes so aware.

Penalty: 200 penalty units.

(5) A port facility operator commits an offence if:

(a) the port facility operator becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on a maritime asset; and

(b) the port facility operator fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 72 hours, after the port facility operator becomes so aware.

Penalty: 200 penalty units.

(6) Subsections (4) and (5) do not apply in relation to a report that must be made to a particular person or body if:

(a) the port facility operator believes, on reasonable grounds, that the person or body is already aware of the incident; or

(b) the port facility operator has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(7) Subsections (4) and (5) are offences of strict liability.

35 Paragraph 174A(1)(a)

After "maritime transport or offshore facility security incident", insert "(other than a cyber security incident)".

36 At the end of section 174A

Add:

Cyber security incidents

(4) An offshore facility operator commits an offence if:

(a) the offshore facility operator becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of a maritime asset; and

(b) the offshore facility operator fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 12 hours, after the offshore facility operator becomes so aware.

Penalty: 200 penalty units.

(5) An offshore facility operator commits an offence if:

(a) the offshore facility operator becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on a maritime asset; and

(b) the offshore facility operator fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 72 hours, after the offshore facility operator becomes so aware.

Penalty: 200 penalty units.

(6) Subsections (4) and (5) do not apply in relation to a report that must be made to a particular person or body if:

(a) the offshore facility operator believes, on reasonable grounds, that the person or body is already aware of the incident; or

(b) the offshore facility operator has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(7) Subsections (4) and (5) are offences of strict liability.

37 Paragraph 175(1)(a)

After "maritime transport or offshore facility security incident", insert "(other than a cyber security incident)".

38 After subsection 175(3)

Insert:

Cyber security incidents

(3A) A person with incident reporting responsibilities commits an offence if:

(a) the person becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of a maritime asset; and

(b) the person fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 12 hours, after the person becomes so aware.

Penalty:

(a) for a person with incident reporting responsibilities who is a maritime industry participant—100 penalty units; and

(b) for any other person with incident reporting responsibilities—50 penalty units.

(3B) A person with incident reporting responsibilities commits an offence if:

(a) the person becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on a maritime asset; and

(b) the person fails to report the incident to:

(i) the Secretary; and

(ii) the Australian Signals Directorate;

as soon as possible, and in any event within 72 hours, after the person becomes so aware.

Penalty:

(a) for a person with incident reporting responsibilities who is a maritime industry participant—100 penalty units; and

(b) for any other person with incident reporting responsibilities—50 penalty units.

(3C) Subsections (3A) and (3B) do not apply in relation to a report that must be made to a particular person or body (the ***person or body to be notified***) if:

(a) the person with incident reporting responsibilities believes, on reasonable grounds, that the person or body to be notified is already aware of the incident; or

(b) the person with incident reporting responsibilities has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(3D) Subsections (3A) and (3B) are offences of strict liability.

39 Paragraph 176(1)(a)

After "maritime transport or offshore facility security incident", insert "(other than a cyber security incident)".

40 At the end of section 176

Add:

Cyber security incidents

(4) An employee of a maritime industry participant commits an offence if:

(a) the employee becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a significant impact on the availability of a maritime asset; and

(b) the employee fails to report the incident to the maritime industry participant as soon as possible, and in any event within 12 hours, after the employee becomes so aware.

Penalty: 50 penalty units.

(5) An employee of a maritime industry participant commits an offence if:

(a) the employee becomes aware of a maritime transport or offshore facility security incident that:

(i) is a cyber security incident; and

(ii) has had, is having, or is likely to have a relevant impact on a maritime asset; and

(b) the employee fails to report the incident to the maritime industry participant as soon as possible, and in any event within 72 hours, after the employee becomes so aware.

Penalty: 50 penalty units.

(6) Subsections (4) and (5) do not apply if the employee has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

(7) Subsections (4) and (5) are offences of strict liability.

41 Subsection 177(1)

After "maritime transport or offshore facility security incidents", insert "(other than cyber security incidents)".

42 Subsection 178(1)

After "maritime transport or offshore facility security incidents", insert "(other than cyber security incidents)".

43 Subsection 179(1)

After "maritime transport or offshore facility security incidents", insert "(other than cyber security incidents)".

44 Subsection 179A(1)

After "maritime transport or offshore facility security incidents", insert "(other than cyber security incidents)".

45 Subsection 180(1)

After "maritime transport or offshore facility security incidents", insert "(other than cyber security incidents)".

46 Subsection 181(1)

After "maritime transport or offshore facility security incidents", insert "(other than cyber security incidents)".

47 Application—security incidents

(1) The amendments of Part 6 of the *Aviation Transport Security Act 2004* made by this Part apply in relation to a security incident that occurs after the commencement of this item.

(2) The amendments of Part 9 of the *Maritime Transport and Offshore Facilities Security Act 2003* made by this Part apply in relation to a security incident that occurs after the commencement of this item.

Part 2—Security assessments

Aviation Transport Security Act 2004

48 Subsection 3(1)

After "aviation", insert "and operational interference with aviation".

49 Section 4 (paragraph beginning "This Act establishes")

After "aviation", insert "and operational interference with aviation".

50 Section 4 (paragraph beginning "Part 2")

After "operations", insert ", and may also deal with safeguarding against unlawful interference with aviation and operational interference with aviation".

51 Section 9

Insert:

operational interference with aviation has the meaning given by section 10AA.

operation of an aviation industry participant means the operation of the participant in the participant's capacity as an aviation industry participant.

relevant interference has the meaning given by section 9F.

52 Before Division 5 of Part 1

Insert:

Division 4B—Relevant interference

9F Meaning of *relevant interference*

(1) Each of the following is a ***relevant interference*** with an asset:

(a) interference (whether direct or indirect) with the availability of the asset;

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

(2) Each of the following is a ***relevant interference*** with the operation of an aviation industry participant:
(a) interference (whether direct or indirect) with the availability of the operation of the participant;
(b) interference (whether direct or indirect) with the integrity of the operation of the participant;
(c) interference (whether direct or indirect) with the reliability of the operation of the participant;
(d) interference (whether direct or indirect) with the confidentiality of information relating to the operation of the participant.

53 After Division 5 of Part 1

Insert:

Division 5A—Operational interference with aviation

10AA Meaning of *operational interference with aviation*

(1) For the purposes of this Act, ***operational interference with aviation*** means:
(a) committing, or attempting to commit, an act that results in a relevant interference with the operation of an aviation industry participant; or
(b) committing, or attempting to commit, an act that results in a relevant interference with an aviation asset; or

(c) the occurrence of a hazard that results in a relevant interference with the operation of an aviation industry participant; or

(d) the occurrence of a hazard that results in a relevant interference with an aviation asset.

(2) However, ***operational interference with aviation*** does not include any of the following:

(a) unlawful interference with aviation;

(b) lawful advocacy, protest, dissent or industrial action.

54 Section 11 (after the paragraph beginning "If the Secretary is satisfied")

Insert:

> An aviation industry participant that has a transport security program (other than a program under Division 6) may be required to give the Secretary an annual statement of compliance for the program. This is dealt with in Division 7.

55 After subsection 16(2)

Insert:

(2A) A transport security program for an aviation industry participant must:

(a) include a security assessment for:

(i) the participant's operation; or

(ii) if the participant has more than one program—the operations or locations covered by the program; and

(b) set out the participant's measures and procedures for addressing the outcomes of the security assessment included in the program; and

(c) set out the participant's measures and procedures for complying with the minimum requirements (if any) for the participant prescribed by the regulations for the purposes of subsection (2D).

(2B) The security assessment under paragraph (2A)(a) must:

(a) take into account any documents required in writing by the Secretary to be taken into account; and
(b) address any matters prescribed by the regulations for the purposes of this paragraph.

(2C) Regulations made for the purposes of paragraph (2B)(b) may prescribe matters for one or more of the following:
(a) each security assessment;
(b) each security assessment for a particular kind of aviation industry participant;
(c) each security assessment for a particular class of a particular kind of aviation industry participant.

(2D) The regulations may, for the purpose of safeguarding against unlawful interference with aviation or operational interference with aviation, prescribe minimum requirements for one or more of the following:
(a) all aviation industry participants;
(b) a particular kind of aviation industry participant;
(c) a particular class of a particular kind of aviation industry participant.

56 At the end of section 16

Add:

(4) The regulations may prescribe matters that:
(a) relate to safeguarding against:
(i) unlawful interference with aviation; or
(ii) operational interference with aviation; and
(b) must be dealt with in one or more of the following:
(i) each transport security program;
(ii) each transport security program for a particular kind of aviation industry participant;
(iii) each transport security program for a particular class of a particular kind of aviation industry participant.

(5) Subsection (4) does not limit subsection (3).

Incorporation by reference

(6) Despite subsection 14(2) of the *Legislation Act 2003*, regulations made for the purposes of this section may make provision in relation to a matter by applying, adopting or incorporating, with or without modification, any matter contained in a document as in force or existing from time to time.

57 After section 25

Insert:

25A Cancelling for failure to provide statement of compliance

If:

(a) a transport security program for an aviation industry participant is in force; and

(b) the participant fails to give the Secretary a statement of compliance for the program in accordance with section 26AB;

the Secretary may, by written notice given to the participant, cancel the approval of the program.

58 After subsection 26C(1)

Insert:

(1A) A transport security program that is given to an aviation industry participant under section 26B may include a security assessment for the participant's operation.

(1B) A transport security program that is given to an aviation industry participant under section 26B may set out the measures and procedures to be undertaken or implemented by the participant under the program for the purposes of safeguarding against:

(a) unlawful interference with aviation; or

(b) operational interference with aviation.

59 At the end of Part 2

Add:

Division 7—Statement of compliance for programs

26AA Application of this Division

This Division applies to a transport security program other than a transport security program given by the Secretary under Division 6.

26AB Annual statement of compliance for programs

(1) If a transport security program for an aviation industry participant is in force on a day (the ***anniversary day***) that is an anniversary of the day the program came into force, the participant must give the Secretary a statement of compliance for the program in accordance with this section.

(2) The participant must give the statement of compliance for the program to the Secretary within 90 days after the anniversary day.

(3) The statement of compliance for the program must:

(a) include whichever of the following statements is applicable:

(i) if the security assessment included in the program is up to date at the end of the anniversary day—a statement to that effect;

(ii) if the security assessment included in the program is not up to date at the end of the anniversary day—a statement to that effect; and

(b) include whichever of the following statements is applicable:

(i) if the measures and procedures set out in the program, as required by paragraphs 16(2A)(b) and (c), are up to date at the end of the anniversary day—a statement to that effect;

(ii) if the measures and procedures set out in the program, as required by paragraphs 16(2A)(b) and (c), are not up to date at the end of the anniversary day—a statement to that effect; and

(c) include any other statement or information prescribed by the regulations for the purposes of this paragraph.

(4) For the purposes of Division 5, a transport security program for an aviation industry participant is taken not to adequately address the relevant requirements under Division 4 if:

(a) the security assessment included in the program is not up to date; or

(b) the participant's measures and procedures set out in the program, as required by paragraphs 16(2A)(b) and (c), are not up to date.

26AC Participants required to provide statement of compliance

(1) An aviation industry participant commits an offence if:

(a) a transport security program for the participant is in force; and

(b) the participant fails to give the Secretary a statement of compliance for the program in accordance with section 26AB.

Penalty:

(a) for an airport operator or an aircraft operator—300 penalty units; and

(b) for an aviation industry participant, other than an airport operator or an aircraft operator—100 penalty units.

(2) Subsection (1) does not apply if the participant has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

(3) Subsection (1) is an offence of strict liability.

60 Subsection 44C(1)

After "safeguarding against unlawful interference with aviation", insert ", safeguarding against operational interference with aviation".

61 Subsection 44C(1)

Omit "(or both)".

62 At the end of subsection 44C(2)

Add:

; (k) security programs for known consignors, regulated air cargo agents or accredited air cargo agents.

63 After subsection 44C(3A)

Insert:

(3B) To avoid doubt, regulations made for the purposes of paragraph (2)(k) may prescribe matters that may, or must, be included in a security program for a known consignor, regulated air cargo agent or accredited air cargo agent.

(3C) Despite subsection 14(2) of the *Legislation Act 2003*, regulations made for the purposes of paragraph (2)(k) may make provision in relation to a matter by applying, adopting or incorporating, with or without modification, any matter contained in a document as in force or existing from time to time.

64 Paragraph 126(1)(d)

After "section 25", insert ", 25A".

65 Application—transport security programs

(1) Subsections 16(2A) and (2B) of the *Aviation Transport Security Act 2004*, as inserted by this Part, apply in relation to a transport security program for an aviation industry participant if:

(a) the participant gives the program to the Secretary under section 18 of that Act after the commencement of this item; or

(b) the participant gives a copy of the program to the Secretary under section 22 of that Act after the commencement of this item; or

(c) the participant gives the program to the Secretary in compliance with a notice that was given under section 23 of that Act after the commencement of this item.

(2) Despite subitem (1), in determining, for the purposes of sections 21, 23, 23A and 25 of the *Aviation Transport Security Act 2004*, whether a transport security program adequately addresses the relevant requirements under Division 4 of Part 2 of that Act, assume that subsections 16(2A) and (2B) of that Act, as inserted by this Part, apply in relation to the program.

(3) The amendment of section 26C of the *Aviation Transport Security Act 2004* made by this Part applies in relation to a transport security program if the program is given to an aviation industry participant under section 26B of that Act after the commencement of this item.

66 Application—statements of compliance

Section 26AB of the *Aviation Transport Security Act 2004*, as inserted by this Part, applies in relation to a transport security program for an aviation industry participant if:

(a) the participant gives the program to the Secretary under section 18 of that Act after the commencement of this item; or

(b) the participant gives a copy of the program to the Secretary under section 22 of that Act after the commencement of this item; or

(c) the participant gives the program to the Secretary in compliance with a notice that was given under section 23 of that Act after the commencement of this item.

Maritime Transport and Offshore Facilities Security Act 2003

67 Subsection 3(1)

After "facilities", insert "or operational interference with maritime transport or offshore facilities".

68 Paragraph 3(4)(b)

Repeal the paragraph, substitute:

(b) the risk of unlawful interference with maritime transport or offshore facilities is reduced without undue disruption to trade;

69 Section 4 (paragraph beginning "This Act establishes")

After "facilities", insert "and operational interference with maritime transport or offshore facilities".

70 Section 10

Insert:

operational interference with maritime transport or offshore facilities has the meaning given by section 11A.

operation of a maritime industry participant means the operation of the participant in the participant's capacity as a maritime industry participant.

relevant interference has the meaning given by section 10F.

71 Before Division 5 of Part 1

Insert:

Division 4B—Relevant interference

10F Meaning of *relevant interference*

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

(2) Each of the following is a ***relevant interference*** with the operation of a maritime industry participant:
  (a) interference (whether direct or indirect) with the availability of the operation of the participant;
  (b) interference (whether direct or indirect) with the integrity of the operation of the participant;

(c) interference (whether direct or indirect) with the reliability of the operation of the participant;
(d) interference (whether direct or indirect) with the confidentiality of information relating to the operation of the participant.

72 After Division 5 of Part 1

Insert:

Division 5A—Operational interference with maritime transport or offshore facilities

11A Meaning of *operational interference with maritime transport or offshore facilities*

(1) For the purposes of this Act, ***operational interference with maritime transport or offshore facilities*** means:
(a) committing, or attempting to commit, an act that results in a relevant interference with the operation of a maritime industry participant; or
(b) committing, or attempting to commit, an act that results in a relevant interference with a maritime asset; or
(c) the occurrence of a hazard that results in a relevant interference with the operation of a maritime industry participant; or
(d) the occurrence of a hazard that results in a relevant interference with a maritime asset.

(2) However, ***operational interference with maritime transport or offshore facilities*** does not include any of the following:
(a) unlawful interference with maritime transport or offshore facilities;
(b) lawful advocacy, protest, dissent or industrial action.

73 Section 41 (after the paragraph beginning "The approval of maritime")

Insert:

Annual statements of compliance for maritime security plans are dealt with in Division 6.

74 After paragraph 47(1)(a)

Insert:

(aa) set out the participant's measures and procedures for addressing the outcomes of the security assessment included in the plan; and

(ab) set out the participant's measures and procedures for complying with the minimum requirements (if any) for the participant prescribed by the regulations for the purposes of subsection (4); and

(ac) set out how the participant will respond to maritime transport or offshore facility security incidents; and

75 At the end of section 47

Add:

(3) Regulations made for the purposes of paragraph (2)(b) may prescribe matters for one or more of the following:

(a) each security assessment;

(b) each security assessment for a particular kind of maritime industry participant;

(c) each security assessment for a particular class of a particular kind of maritime industry participant.

(4) The regulations may prescribe minimum requirements for one or more of the following:

(a) all maritime industry participants;

(b) a particular kind of maritime industry participant;

(c) a particular class of a particular kind of maritime industry participant;

for the purpose of safeguarding against:

(d) unlawful interference with maritime transport or offshore facilities; or

(e) operational interference with maritime transport of offshore facilities.

Incorporation by reference

(5) Despite subsection 14(2) of the *Legislation Act 2003*, regulations made for the purposes of this section and section 48 of this Act may make provision in relation to a matter by applying, adopting or incorporating, with or without modification, any matter contained in a document as in force or existing from time to time.

76 Section 48

Before "The regulations", insert "(1)".

77 At the end of section 48

Add:

(2) The regulations may prescribe matters that:
  (a) relate to safeguarding against:
    (i) unlawful interference with maritime transport or offshore facilities; or
    (ii) operational interference with maritime transport or offshore facilities; and
  (b) must be dealt with in one or more of the following:
    (i) each maritime security plan;
    (ii) each maritime security plan for a particular kind of maritime industry participant;
    (iii) each maritime security plan for a particular class of a particular kind of maritime industry participant.

(3) Subsection (2) does not limit subsection (1).

78 After section 57

Insert:

57A Cancelling for failure to provide statement of compliance

If:
  (a) a maritime security plan for a maritime industry participant is in force; and
  (b) the participant fails to give the Secretary a statement of compliance for the plan in accordance with section 59A;

the Secretary may, by written notice given to the participant, cancel the approval of the plan.

79 At the end of Part 3

Add:

Division 6—Statement of compliance for plans

59A Annual statement of compliance for maritime security plans

(1) If a maritime security plan for a maritime industry participant is in force on a day (the ***anniversary day***) that is an anniversary of the day the plan came into force, the participant must give the Secretary a statement of compliance for the plan in accordance with this section.

(2) The participant must give the statement of compliance for the plan to the Secretary within 90 days after the anniversary day.

(3) The statement of compliance for the plan must:

(a) include whichever of the following statements is applicable:

(i) if the security assessment included in the plan is up to date at the end of the anniversary day—a statement to that effect;

(ii) if the security assessment included in the plan is not up to date at the end of the anniversary day—a statement to that effect; and

(b) include whichever of the following statements is applicable:

(i) if the measures and procedures set out in the plan, as required by paragraphs 47(1)(aa) and (ab), are up to date at the end of the anniversary day—a statement to that effect;

(ii) if the measures and procedures set out in the plan, as required by paragraphs 47(1)(aa) and (ab), are not up to date at the end of the anniversary day—a statement to that effect; and

(c) include any other statement or information prescribed by the regulations for the purposes of this paragraph.

(4) For the purposes of Division 5, a maritime security plan for a maritime industry participant is taken not to adequately address the relevant requirements under Division 4 if:
  (a) the security assessment included in the plan is not up to date; or
  (b) the measures and procedures set out in the plan, as required by paragraphs 47(1)(aa) and (ab), are not up to date.

59B Participants required to provide statement of compliance

(1) A maritime industry participant commits an offence if:
  (a) a maritime security plan for the participant is in force; and
  (b) the participant fails to give the Secretary a statement of compliance for the plan in accordance with section 59A.

Penalty:
  (a) for a port operator or port facility operator—200 penalty units; and
  (b) for any other maritime industry participant—100 penalty units.

(2) Subsection (1) does not apply if the participant has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

(3) Subsection (1) is an offence of strict liability.

80 Section 60 (after the paragraph beginning "The approval of ship")

Insert:

> Annual statements of compliance for ship security plans are dealt with in Division 5A.

81 After paragraph 66(1)(a)

Insert:

(aa) set out the ship operator's measures and procedures for addressing the results of the security assessment included in the plan; and

(ab) set out the ship operator's measures and procedures for complying with the minimum requirements (if any) for the ship prescribed by the regulations for the purposes of subsection (4); and

(ac) set out how the ship operator will respond to maritime transport or offshore facility security incidents that affect the ship; and

82 At the end of section 66

Add:

(3) Regulations made for the purposes of paragraph (2)(b) may prescribe matters for one or more of the following:

(a) each security assessment;

(b) each security assessment for a particular kind of ship;

(c) each security assessment for a particular class of a particular kind of ship.

(4) The regulations may prescribe minimum requirements for one or more of the following:

(a) all regulated Australian ships;

(b) a particular kind of regulated Australian ship;

(c) a particular class of a particular kind of regulated Australian ship;

for the purpose of safeguarding against:

(d) unlawful interference with maritime transport or offshore facilities; or

(e) operational interference with maritime transport of offshore facilities.

Incorporation by reference

(5) Despite subsection 14(2) of the *Legislation Act 2003*, regulations made for the purposes of this section and section 67 of this Act may make provision in relation to a matter by applying, adopting

or incorporating, with or without modification, any matter contained in a document as in force or existing from time to time.

83 Section 67

Before "The regulations", insert "(1)".

84 At the end of section 67

Add:

(2) The regulations may prescribe matters that:
  (a) relate to safeguarding against:
    (i) unlawful interference with maritime transport or offshore facilities; or
    (ii) operational interference with maritime transport or offshore facilities; and
  (b) must be dealt with in one or more of the following:
    (i) each ship security plan;
    (ii) each ship security plan for a particular kind of ship;
    (iii) each ship security plan for a particular class of a particular kind of ship.

(3) Subsection (2) does not limit subsection (1).

85 After section 76

Insert:

76A Cancelling for failure to provide statement of compliance

If:
  (a) a ship security plan for a regulated Australian ship is in force; and
  (b) the ship operator for the ship fails to give the Secretary a statement of compliance for the plan in accordance with section 78A;

the Secretary may, by written notice given to the ship operator, cancel the approval of the plan.

86 After Division 5 of Part 4

Insert:

Division 5A—Statement of compliance for plans

78A Annual statement of compliance for ship security plans

(1) If a ship security plan for a regulated Australian ship is in force on a day (the ***anniversary day***) that is an anniversary of the day the plan came into force, the ship operator for the ship must give the Secretary a statement of compliance for the plan in accordance with this section.

(2) The ship operator must give the statement of compliance for the plan to the Secretary within 90 days after the anniversary day.

(3) The statement of compliance for the plan must:

(a) include whichever of the following statements is applicable:

(i) if the security assessment included in the plan is up to date at the end of the anniversary day—a statement to that effect;

(ii) if the security assessment included in the plan is not up to date at the end of the anniversary day—a statement to that effect; and

(b) include whichever of the following statements is applicable:

(i) if the measures and procedures set out in the plan, as required by paragraphs 66(1)(aa) and (ab), are up to date at the end of the anniversary day—a statement to that effect;

(ii) if the measures and procedures set out in the plan, as required by paragraphs 66(1)(aa) and (ab), are not up to date at the end of the anniversary day—a statement to that effect; and

(c) include any other statement or information prescribed by the regulations for the purposes of this paragraph.

(4) For the purposes of Division 5, a ship security plan for a regulated Australian ship is taken not to adequately address the relevant requirements under Division 4 if:

(a) the security assessment included in the plan is not up to date; or

(b) the measures and procedures set out in the plan, as required by paragraphs 66(1)(aa) and (ab), are not up to date.

78B Ship operators required to provide statement of compliance

(1) The ship operator for a regulated Australian ship commits an offence if:

(a) a ship security plan for the ship is in force; and

(b) the operator fails to give the Secretary a statement of compliance for the plan in accordance with section 78A.

Penalty: 200 penalty units.

(2) Subsection (1) does not apply if the operator has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

(3) Subsection (1) is an offence of strict liability.

87 Section 100A (after the paragraph beginning "The approval of offshore")

Insert:

> Annual statements of compliance for offshore security plans are dealt with in Division 6.

88 After paragraph 100G(1)(a)

Insert:

(aa) set out the participant's measures and procedures for addressing the outcomes of the security assessment included in the plan; and

(ab) set out the participant's measures and procedures for complying with the minimum requirements (if any) for the participant prescribed by the regulations for the purposes of subsection (4); and

(ac) set out how the participant will respond to maritime transport or offshore facility security incidents; and

89 At the end of section 100G

Add:

(3) Regulations made for the purposes of paragraph (2)(b) may prescribe matters for one or more of the following:
  (a) each security assessment;
  (b) each security assessment for a particular kind of offshore industry participant;
  (c) each security assessment for a particular class of a particular kind of offshore industry participant.

(4) The regulations may prescribe minimum requirements for one or more of the following:
  (a) all offshore industry participants;
  (b) a particular kind of offshore industry participant;
  (c) a particular class of a particular kind of offshore industry participant;

for the purpose of safeguarding against:
  (d) unlawful interference with maritime transport or offshore facilities; or
  (e) operational interference with maritime transport of offshore facilities.

Incorporation by reference

(5) Despite subsection 14(2) of the *Legislation Act 2003*, regulations made for the purposes of this section and section 100H of this Act may make provision in relation to a matter by applying, adopting or incorporating, with or without modification, any matter contained in a document as in force or existing from time to time.

90 Section 100H

Before "The regulations", insert "(1)".

91 At the end of section 100H

Add:

(2) The regulations may prescribe matters that:
(a) relate to safeguarding against:
(i) unlawful interference with maritime transport or offshore facilities; or
(ii) operational interference with maritime transport or offshore facilities; and
(b) must be dealt with in one or more of the following:
(i) each offshore security plan;
(ii) each offshore security plan for a particular kind of offshore industry participant;
(iii) each offshore security plan for a particular class of a particular kind of offshore industry participant.

(3) Subsection (2) does not limit subsection (1).

92 After section 100Q

Insert:

100QA Cancelling for failure to provide statement of compliance

If:
(a) an offshore security plan for an offshore industry participant is in force; and
(b) the participant fails to give the Secretary a statement of compliance for the plan in accordance with section 100TA;

the Secretary may, by written notice given to the participant, cancel the approval of the plan.

93 At the end of Part 5A

Add:

Division 6—Statement of compliance for plans

100TA Annual statement of compliance for offshore security plans

(1) If an offshore security plan for an offshore industry participant is in force on a day (the ***anniversary day***) that is an anniversary of the day the plan came into force, the participant must give the

Secretary a statement of compliance for the plan in accordance with this section.

(2) The participant must give the statement of compliance for the plan to the Secretary within 90 days after the anniversary day.

(3) The statement of compliance for the plan must:
  (a) include whichever of the following statements is applicable:
    (i) if the security assessment included in the plan is up to date at the end of the anniversary day—a statement to that effect;
    (ii) if the security assessment included in the plan is not up to date at the end of the anniversary day—a statement to that effect; and
  (b) include whichever of the following statements is applicable:
    (i) if the measures and procedures set out in the plan, as required by paragraphs 100G(1)(aa) and (ab), are up to date at the end of the anniversary day—a statement to that effect;
    (ii) if the measures and procedures set out in the plan, as required by paragraphs 100G(1)(aa) and (ab), are not up to date at the end of the anniversary day—a statement to that effect; and
  (c) include any other statement or information prescribed by the regulations for the purposes of this paragraph.

(4) For the purposes of Division 5, an offshore security plan for an offshore industry participant is taken not to adequately address the relevant requirements under Division 4 if:
  (a) the security assessment included in the plan is not up to date; or
  (b) the participant's measures and procedures set out in the plan, as required by paragraphs 100G(1)(aa) and (ab), are not up to date.

100TB Participant required to provide statement of compliance

(1) An offshore industry participant commits an offence if:
  (a) an offshore security plan for the participant is in force; and

(b) the participant fails to give the Secretary a statement of compliance for the plan in accordance with section 100TA.

Penalty:

(a) for an offshore facility operator—200 penalty units; and

(b) for any other offshore industry participant—100 penalty units.

(2) Subsection (1) does not apply if the participant has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

(3) Subsection (1) is an offence of strict liability.

94 Paragraph 201(d)

After "section 57,", insert "57A,".

95 Paragraph 201(d)

After "76,", insert "76A,".

96 Paragraph 201(d)

After "100Q", insert ", 100QA".

97 Application—maritime security plans

(1) The amendments of subsections 3(4) and 47(1) of the *Maritime Transport and Offshore Facilities Security Act 2003* made by this Part apply in relation to a maritime security plan for a maritime industry participant if:

(a) the participant gives the plan to the Secretary under section 50 of that Act after the commencement of this item; or

(b) the participant gives a copy of the plan to the Secretary under section 54 of that Act after the commencement of this item; or

(c) the participant gives the plan to the Secretary in compliance with a notice that was given under section 55 of that Act after the commencement of this item.

(2) Despite subitem (1), in determining, for the purposes of sections 53, 55 and 57 of the *Maritime Transport and Offshore Facilities Security Act 2003*, whether a maritime security plan adequately addresses the relevant requirements under Division 4 of Part 3 of that Act, assume that the amendments of subsections 3(4) and 47(1) of that Act made by this Part apply in relation to the plan.

98 Application—ship security plans

(1) The amendments of subsections 3(4) and 66(1) of the *Maritime Transport and Offshore Facilities Security Act 2003* made by this Part apply in relation to a ship security plan for a regulated Australian ship if:

(a) the ship operator gives the plan to the Secretary under section 69 of that Act after the commencement of this item; or

(b) the ship operator gives a copy of the plan to the Secretary under section 73 of that Act after the commencement of this item; or

(c) the ship operator gives the plan to the Secretary in compliance with a notice that was given under section 74 of that Act after the commencement of this item.

(2) Despite subitem (1), in determining, for the purposes of sections 72, 74 and 76 of the *Maritime Transport and Offshore Facilities Security Act 2003*, whether a ship security plan adequately addresses the relevant requirements under Division 4 of Part 4 of that Act, assume that the amendments of subsections 3(4) and 66(1) of that Act made by this Part apply in relation to the plan.

99 Application—offshore security plans

(1) The amendments of subsections 3(4) and 100G(1) of the *Maritime Transport and Offshore Facilities Security Act 2003* made by this Part apply in relation to an offshore security plan for an offshore industry participant if:

(a) the participant gives the plan to the Secretary under section 100J of that Act after the commencement of this item; or

(b) the participant gives a copy of the plan to the Secretary under section 100N of that Act after the commencement of this item; or

(c) the participant gives the plan to the Secretary in compliance with a notice that was given under section 100O of that Act after the commencement of this item.

(2) Despite subitem (1), in determining, for the purposes of sections 100M, 100O and 100Q of the *Maritime Transport and Offshore Facilities Security Act 2003*, whether an offshore security plan adequately addresses the relevant requirements under Division 4 of Part 5A of that Act, assume that the amendments of subsections 3(4) and 100G(1) of that Act made by this Part apply in relation to the plan.

100 Application—statements of compliance

Statements of compliance for maritime security plans

Section 59A of the *Maritime Transport and Offshore Facilities Security Act 2003*, as inserted by this Part, applies in relation to a maritime security plan for a maritime industry participant if:

(a) the participant gives the plan to the Secretary under section 50 of that Act after the commencement of this item; or

(b) the participant gives a copy of the plan to the Secretary under section 54 of that Act after the commencement of this item; or

(c) the participant gives the plan to the Secretary in compliance with a notice that was given under section 55 of that Act after the commencement of this item.

Statements of compliance for ship security plans

Section 78A of the *Maritime Transport and Offshore Facilities Security Act 2003*, as inserted by this Part, applies in relation to a ship security plan for a regulated Australian ship if:

(a) the ship operator gives the plan to the Secretary under section 69 of that Act after the commencement of this item; or

(b) the ship operator gives a copy of the plan to the Secretary under section 73 of that Act after the commencement of this item; or

(c) the ship operator gives the plan to the Secretary in compliance with a notice that was given under section 74 of that Act after the commencement of this item.

Statements of compliance for offshore security plans

Section 100TA of the *Maritime Transport and Offshore Facilities Security Act 2003*, as inserted by this Part, applies in relation to an offshore security plan for an offshore industry participant if:

(a) the participant gives the plan to the Secretary under section 100J of that Act after the commencement of this item; or

(b) the participant gives a copy of the plan to the Secretary under section 100N of that Act after the commencement of this item; or

(c) the participant gives the plan to the Secretary in compliance with a notice that was given under section 100O of that Act after the commencement of this item.

Part 3—Powers of security inspectors

Aviation Transport Security Act 2004

101 Section 9

Insert:

> ***connect***, in relation to equipment, includes connection otherwise than by means of physical contact, for example, a connection by means of radiocommunication.

102 Section 76

Omit "this Act.", substitute "this Act, or whether there is a flaw or vulnerability in an aviation security system.".

103 At the end of subsection 79(1)

Add:

; (c) identifying the existence, or extent, of:

(i) a flaw in an aviation security system; or

(ii) a vulnerability in an aviation security system.

104 Paragraph 79(2)(h)

Repeal the paragraph (not including the note), substitute:

(h) test a security system for a place or vehicle mentioned in paragraph (a) or (b) in accordance with the requirements prescribed by the regulations for the purposes of this paragraph, including by:

(i) using an item, test weapon or vehicle to test its detection; and

(ii) operating, or connecting to, equipment (including electronic equipment) located in the place or vehicle or at any other place in Australia.

105 After subsection 79(2A)

Insert:

(2B) For the purposes of paragraph (2)(h), it is immaterial whether the testing of a security system for a place or vehicle mentioned in paragraph (2)(a) or (b) is done:

(a) in the place or vehicle; or

(b) at any other place in Australia.

106 Paragraph 79(3A)(f)

Repeal the paragraph, substitute:

(f) a power covered by subparagraph (2)(h), to the extent that it relates to subparagraph (2)(b)(i).

107 After paragraph 80(1)(b)

Insert:

; (c) identifying the existence, or extent, of:

(i) a flaw in an aviation security system; or

(ii) a vulnerability in an aviation security system.

108 Paragraph 80(2)(f)

Repeal the paragraph (not including the note), substitute:

(f) test a security system for the aircraft in accordance with the requirements prescribed by the regulations for the purposes of this paragraph, including by:

(i) using an item, test weapon or vehicle to test its detection; and

(ii) operating, or connecting to, equipment (including electronic equipment) located in the aircraft or at any other place in Australia.

109 Subsection 80(2A)

Repeal the subsection, substitute:

(2A) However, a power under paragraph (2)(f) to test a security system for an aircraft:

(a) must not be exercised unless regulations prescribing requirements for conducting tests of security systems have been made for the purposes of that paragraph and are in force; and

(b) must not be exercised while passengers are on board, boarding or disembarking from the aircraft.

110 After subsection 80(2A)

Insert:

(2B) For the purposes of paragraph (2)(f), it is immaterial whether the testing of a security system for an aircraft is done:

(a) in the aircraft; or

(b) at any other place in Australia.

111 Transitional—requirements for testing security systems

(1) Regulations made for the purposes of paragraph 79(2)(h) of the *Aviation Transport Security Act 2004* that were in force immediately before the commencement of this item continue in force (and may be dealt with) as if they had been made for the purposes of paragraph 79(2)(h) of that Act, as substituted by this Part.

(2) Regulations made for the purposes of paragraph 80(2)(f) of the *Aviation Transport Security Act 2004* that were in force immediately before the commencement of this item continue in force (and may be dealt with) as if they had been made for the purposes of paragraph 80(2)(f) of that Act, as substituted by this Part.

Maritime Transport and Offshore Facilities Security Act 2003

112 Section 10

Insert:

connect, in relation to equipment, includes connection otherwise than by means of physical contact, for example, a connection by means of radiocommunication.

113 Section 10 (paragraph (b) of the definition of *prohibited item*)

Omit "prescribed in the regulations for the purposes of this definition", substitute "specified in an instrument in force under section 10A".

114 Section 10

Insert:

test weapon means:

(a) a weapon of a kind that is a replica or an imitation of another weapon; or

(b) a weapon that, as a result of a modification, is not capable of operating as a functional weapon; or

(c) a thing prescribed by the regulations to be a test weapon.

115 At the end of Division 4 of Part 1

Add:

10A Prohibited items

The Minister may, by legislative instrument, make a determination specifying items for the purposes of paragraph (b) of the definition of ***prohibited item*** in section 10.

116 Section 135

Omit "this Act.", substitute "this Act, and to identify flaws or vulnerabilities in maritime security systems.".

117 At the end of subsection 139(1)

Add:

; (c) identifying the existence, or extent, of:

(i) a flaw in a maritime security system; or

(ii) a vulnerability in a maritime security system.

118 At the end of subsection 139(2)

Add:

; (g) test a security system for the ship in accordance with the requirements prescribed by the regulations for the purposes of this paragraph, including by:

(i) using an item, test weapon, vehicle or vessel to test its detection; and

(ii) operating, or connecting to, equipment (including electronic equipment) on the ship or at any other place in Australia.

Note: A maritime security inspector must ensure that the exercise of the power under paragraph (g) does not seriously endanger the health or safety of any person, or the inspector will not be immune from civil or criminal liability (see subsection (4)).

119 After subsection 139(2)

Insert:

(2A) However, a power under paragraph (2)(g) must not be exercised unless regulations prescribing requirements for conducting tests of security systems have been made for the purposes of that paragraph and are in force.

(2B) For the purposes of paragraph (2)(g), it is immaterial whether the testing of a security system for a security regulated ship is done:

(a) on the ship; or

(b) at any other place in Australia.

120 At the end of section 139

Add:

Power to test a security system—immunity

(4) A maritime security inspector is not subject to any civil or criminal liability under a law of the Commonwealth, a State or a Territory in relation to the exercise of a power under paragraph (2)(g) to the extent that the exercise of the power:

(a) is in good faith; and

(b) does not seriously endanger the health or safety of any person; and

(c) does not result in significant loss of, or serious damage to, property.

Note: A defendant bears an evidential burden in relation to the matter in this subsection for a criminal proceeding (see subsection 13.3(3) of the *Criminal Code*).

(5) A person who wishes to rely on subsection (4) in relation to a civil proceeding bears an evidential burden in relation to that matter.

(6) In this section:

evidential burden, in relation to a matter, means the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.

121 At the end of subsection 140A(1)

Add:

; (c) identifying the existence, or extent, of:

(i) a flaw in a maritime security system; or

(ii) a vulnerability in a maritime security system.

122 At the end of subsection 140A(2)

Add:

; (g) test a security system for the facility in accordance with the requirements prescribed by the regulations for the purposes of this paragraph, including by:

(i) using an item, test weapon, vehicle or vessel to test its detection; and

(ii) operating, or connecting to, equipment (including electronic equipment) on the facility or at any other place in Australia.

Note: A maritime security inspector must ensure that the exercise of the power under paragraph (g) does not seriously endanger the health or safety of any person, or the inspector will not be immune from civil or criminal liability (see subsection (5)).

123 After subsection 140A(2)

Insert:

(2A) However, a power under paragraph (2)(g) must not be exercised unless regulations prescribing requirements for conducting tests of security systems have been made for the purposes of that paragraph and are in force.

(2B) For the purposes of paragraph (2)(g), it is immaterial whether the testing of a security system for a security regulated offshore facility is done:

(a) on the facility; or

(b) at any other place in Australia.

124 At the end of section 140A

Add:

Power to test a security system—immunity

(5) A maritime security inspector is not subject to any civil or criminal liability under a law of the Commonwealth, a State or a Territory in relation to the exercise of a power under paragraph (2)(g) to the extent that the exercise of the power:

(a) is in good faith; and

(b) does not seriously endanger the health or safety of any person; and

(c) does not result in significant loss of, or serious damage to, property.

Note: A defendant bears an evidential burden in relation to the matter in this subsection for a criminal proceeding (see subsection 13.3(3) of the *Criminal Code*).

(6) A person who wishes to rely on subsection (5) in relation to a civil proceeding bears an evidential burden in relation to that matter.

(7) In this section:

evidential burden, in relation to a matter, means the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.

125 At the end of subsection 141(1)

Add:

; (c) identifying the existence, or extent, of:

(i) a flaw in a maritime security system; or

(ii) a vulnerability in a maritime security system.

126 At the end of subsection 141(2)

Add:

; (g) test a security system for a place, vehicle or vessel mentioned in paragraph (a) in accordance with the requirements prescribed by the regulations for the purposes of this paragraph, including by:

(i) using an item, test weapon, vehicle or vessel to test its detection; and

(ii) operating, or connecting to, equipment (including electronic equipment) in the place, vehicle or vessel or at any other place in Australia.

Note: A maritime security inspector must ensure that the exercise of the power under paragraph (g) does not seriously endanger the health or safety of any person, or the inspector will not be immune from civil or criminal liability (see subsection (4)).

127 After subsection 141(2)

Insert:

(2A) However, a power under paragraph (2)(g) must not be exercised unless regulations prescribing requirements for conducting tests of security systems have been made for the purposes of that paragraph and are in force.

(2B) For the purposes of paragraph (2)(g), it is immaterial whether the testing of a security system for a place, vehicle or vessel mentioned in paragraph (2)(a) is done:

(a) in the place, vehicle or vessel; or

(b) at any other place in Australia.

128 Subsection 141(3)

Omit "However, in", substitute "In".

129 At the end of section 141

Add:

Power to test a security system—immunity

(4) A maritime security inspector is not subject to any civil or criminal liability under a law of the Commonwealth, a State or a Territory in relation to the exercise of a power under paragraph (2)(g) to the extent that the exercise of the power:

(a) is in good faith; and

(b) does not seriously endanger the health or safety of any person; and

(c) does not result in significant loss of, or serious damage to, property.

Note: A defendant bears an evidential burden in relation to the matter in this subsection for a criminal proceeding (see subsection 13.3(3) of the *Criminal Code*).

(5) A person who wishes to rely on subsection (4) in relation to a civil proceeding bears an evidential burden in relation to that matter.

(6) In this section:

evidential burden, in relation to a matter, means the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.

130 Paragraph 143(1)(b)

After "this Division", insert "(other than the powers mentioned in paragraphs 139(2)(g), 140A(2)(g) and 141(2)(g))".

Part 4—Charging of fees

Aviation Transport Security Act 2004

131 Section 27 (after the paragraph beginning "Regulations under Division 4A")

Insert:

> Regulations under Division 4B may make provision for and in relation to the charging of fees in connection with security passes or other identification systems.

132 After Division 4A of Part 3

Insert:

Division 4B—Charging of fees

38AC Charging of fees related to security passes etc.

(1) The regulations may make provision for and in relation to the charging of fees by a person for activities carried out by, or on behalf of, the person in performing functions or exercising powers under regulations made for the purposes of Division 3, 4 or 4A of this Part in connection with security passes or other identification systems.

(2) Without limiting subsection (1), the regulations may do any of the following:

(a) prescribe a fee by specifying the amount of the fee or a method of working out the fee;

(b) specify that the amount of a fee is the cost incurred by the person in arranging and paying for another person to carry out the relevant activity;

(c) make provision for the charging of fees:

(i) by, or on behalf of, the Commonwealth; or

(ii) by any other person;

(d) make provision for the recovery of fees;

(e) prescribe one or more persons who are liable to pay a specified fee;

(f) prescribe the time when a specified fee is due and payable.

(3) A fee prescribed for the purposes of subsection (1) must not be such as to amount to taxation.

Schedule 2—Amendments commencing immediately after Schedule 1

Maritime Transport and Offshore Facilities Security Act 2003

1 Section 4 (paragraph beginning "Part 5B")

Repeal the paragraph.

2 Section 4 (paragraph beginning "Part 5C")

Repeal the paragraph.

3 Paragraph 6(2)(a)

Repeal the paragraph, substitute:

(a) an offence under subsection 39(1) or 40(1) by a person who is given a direction under section 35 because of the person's presence on, or connection with, a security regulated offshore facility;

4 Paragraph 6(2)(b)

Repeal the paragraph.

5 Paragraph 6(2)(d)

Repeal the paragraph, substitute:

(d) an offence under subsection 121(1), 121(3), 128(1) or 128(3) where the screening point is in, or at the edge of, an offshore security zone;

6 Paragraph 6(2)(e)

Repeal the paragraph.

7 Paragraph 6(2)(i)

Repeal the paragraph, substitute:

(i) an offence under regulations made under section 109, 113D, 119, 126 or 133 where the offence is committed in, or at the edge of:

(i) an offshore security zone; or
(ii) a ship security zone declared under subsection 106(1AA) or (1A).

8 Section 10 (definition of *Australian ship regulated as an offshore facility*)

Repeal the definition.

9 Section 10 (definition of *control direction*)

Omit "or 100ZM(2)".

10 Section 10 (definition of *foreign ship regulated as an offshore facility*)

Repeal the definition.

11 Section 10

Insert:

infrequent overseas voyages test has the meaning given by section 17AA.

12 Section 10 (definition of *interim ISSC*)

Repeal the definition, substitute:

interim ISSC means an interim ISSC given under section 86.

13 Section 10

Insert:

ISSC exemption certificate means a certificate issued under section 89D.

14 Section 10 (definition of *ISSC verified*)

Repeal the definition, substitute:

ISSC verified has the meaning given by subsections 83(1) and (3).

15 Section 10 (definition of *ship regulated as an offshore facility*)

Repeal the definition.

16 Section 10

Insert:

ship security plan exemption certificate means a certificate issued under section 89B.

17 Section 10 (definition of *ship security record*)

Omit "or ship regulated as an offshore facility".

18 Section 10 (definition of *ship security zone*)

After "106(1)", insert ", (1AA)".

19 After paragraph 16(1)(c)

Insert:

(ca) a FPSO; or

(cb) a FSU; or

20 Paragraph 16(2)(a)

Repeal the paragraph, substitute:

(a) a ship that passes the infrequent overseas voyages test (see section 17AA);

21 Subsection 16(3)

Repeal the subsection (including the note).

22 After subparagraph 17(1)(b)(iii)

Insert:

(iiia) a FPSO;

(iiib) a FSU;

23 Paragraph 17(1)(d)

Repeal the paragraph, substitute:

(d) either:

(i) is in, or is intending to proceed to, a port in Australia; or
(ii) is, or is intended to be, connected to the seabed.

24 Subsections 17(2) and (3)

Repeal the subsections (including the note), substitute:

(2) However, a ship of a kind prescribed by the regulations is not a ***regulated foreign ship***.

25 At the end of Division 7 of Part 1

Add:

17AA Infrequent overseas voyages test

A ship passes the ***infrequent overseas voyages test*** if each overseas voyage undertaken by the ship is undertaken in exceptional circumstances.

26 Subsections 17A(2) and (3)

Repeal the subsections.

27 At the end of subsection 17A(4)

Add:

; or (d) a FPSO; or
(e) a FSU.

28 Subsection 17D(1)

Omit "neither a regulated foreign ship, nor a foreign ship regulated as an offshore facility", substitute "not a regulated foreign ship".

29 Subsection 17E(1)

Omit "neither a regulated foreign ship, nor a foreign ship regulated as an offshore facility", substitute "not a regulated foreign ship".

30 Section 20 (paragraph beginning "If maritime security level 2 or 3 is in force for a port")

Omit ", ship regulated as an offshore facility".

31 Section 20 (paragraph beginning "A foreign ship")

Repeal the paragraph.

32 Subsection 22(4)

Repeal the subsection.

33 Paragraph 24(c)

Repeal the paragraph.

34 Paragraph 25(3)(b)

Omit "or is taken to have made such a declaration because of subsection 22(4)".

35 Paragraph 26(ba)

Repeal the paragraph.

36 Subsection 28A(1)

Omit "(and the declaration is not one that, under subsection 22(4), is taken to have been made),".

37 Paragraph 28A(2)(b)

Omit "facility; and", substitute "facility.".

38 Paragraph 28A(2)(c)

Repeal the paragraph.

39 Section 36A

Repeal the section.

40 Paragraph 38(2)(a)

Omit ", or a direction given under section 36A to the offshore facility operator for, or the master of, a ship regulated as an offshore facility".

41 Subsection 39(1)

Omit "or 36A".

42 Subsection 40(1)

Omit "or 36A".

43 After Part 4

Insert:

Part 4A—Exemption certificates for ships that pass the infrequent overseas voyages test

Division 1—Simplified outline of Part

89A Simplified outline of Part

If a ship passes the infrequent overseas voyages test, the Secretary may issue a ship security plan exemption certificate in relation to the ship.

If a ship passes the infrequent overseas voyages test, the Secretary may issue an ISSC exemption certificate in relation to the ship.

Division 2—Exemption certificates for ships that pass the infrequent overseas voyages test

89B Ship security plan exemption certificate

(1) A ship operator for a ship that passes the infrequent overseas voyages test may apply to the Secretary for a certificate (a ***ship security plan exemption certificate***) stating that if:

(a) the ship were a regulated Australian ship; and

(b) the ship operator had applied under section 61A for the ship to be exempt from the operation of Division 2 of Part 4;

the Secretary would have exempted the ship from the operation of that Division in specified circumstances.

Note: For the ***infrequent overseas voyages test***, see section 17AA.

(2) The application must be in accordance with any requirements prescribed by the regulations.

(3) In deciding whether to issue a ship security plan exemption certificate, the Secretary must consider the matters prescribed by the regulations for the purposes of this subsection. The Secretary may consider any other matters that the Secretary considers appropriate.

Secretary's decision

(4) If an application is made to the Secretary, the Secretary must:
  (a) issue a ship security plan exemption certificate in response to the application; or
  (b) refuse to issue such a certificate.

Issue of certificate

(5) If the Secretary issues a ship security plan exemption certificate, the Secretary must give the ship operator a copy of the certificate.

Refusal to issue certificate

(6) If the Secretary refuses to issue a ship security plan exemption certificate, the Secretary must give the ship operator written notice of the refusal (including the reasons for the refusal).

Certificate is not a legislative instrument

(7) A ship security plan exemption certificate is not a legislative instrument.

89C Cancellation of a ship security plan exemption certificate

(1) If there is a ship security plan exemption certificate for a ship, the Secretary may, by written notice given to the ship operator, cancel the certificate.

(2) In deciding whether to cancel a ship security plan exemption certificate, the Secretary must consider the matters prescribed by the regulations for the purposes of this subsection. The Secretary may consider any other matters that the Secretary considers appropriate.

89D ISSC exemption certificate

(1) A ship operator for a ship that passes the infrequent overseas voyages test may apply to the Secretary for a certificate (an ***ISSC exemption certificate***):

(a) stating that if:

(i) the ship were a regulated Australian ship; and

(ii) the ship operator had applied under section 79A for the ship to be exempt from the operation of Division 6 of Part 4;

the Secretary would have exempted the ship from the operation of that Division in specified circumstances; and

(b) stating that the certificate is only valid for a specified voyage.

Note: For the ***infrequent overseas voyages test***, see section 17AA.

(2) The application must be in accordance with any requirements prescribed by the regulations.

(3) In deciding whether to issue an ISSC exemption certificate, the Secretary must consider the matters prescribed by the regulations for the purposes of this subsection. The Secretary may consider any other matters that the Secretary considers appropriate.

Secretary's decision

(4) If an application is made to the Secretary, the Secretary must:

(a) issue an ISSC exemption certificate in response to the application; or

(b) refuse to issue such a certificate.

(5) If the ship is required, by or under the *Navigation Act 2012*, to have a safety certificate of a particular kind when the ship is taken to sea, the Secretary must not issue an ISSC exemption certificate for the ship unless the Secretary is satisfied that the ship has such a safety certificate.

Issue of certificate

(6) If the Secretary issues an ISSC exemption certificate, the Secretary must give the ship operator a copy of the certificate.

Refusal to issue certificate

(7) If the Secretary refuses to issue an ISSC exemption certificate, the Secretary must give the ship operator written notice of the refusal (including the reasons for the refusal).

Certificate is not a legislative instrument

(8) An ISSC exemption certificate is not a legislative instrument.

Deemed voyage

(9) For the purposes of this section, if:

(a) a ship undertakes a voyage in the course of which the ship travels from a port in Australia (the ***departure port***) to a port outside Australia (the ***destination port***); and

(b) the ship undertakes a return voyage in the course of which the ship travels from the destination port to:

(i) the departure port; or

(ii) another port in Australia;

those voyages are taken to be a single voyage.

Specification of voyage

(10) Subsection 33(3AB) of the *Acts Interpretation Act 1901* does not apply to the specification of a voyage in an ISSC exemption certificate.

Note: Subsection 33(3AB) of the *Acts Interpretation Act 1901* deals with specification by class.

89E Cancellation of an ISSC exemption certificate

(1) If there is an ISSC exemption certificate for a ship, the Secretary may, by written notice given to the ship operator, cancel the certificate.

(2) In deciding whether to cancel an ISSC exemption certificate, the Secretary must consider the matters prescribed by the regulations for the purposes of this subsection. The Secretary may consider any other matters that the Secretary considers appropriate.

44 Part 5B

Repeal the Part.

45 Part 5C

Repeal the Part.

46 After subsection 106(1)

Insert:

FPSOs and FSUs

(1AA) The Secretary may, by written notice given to the ship operator for, or the master of, a security regulated ship that is:

(a) a FPSO; or

(b) a FSU;

declare that a ***ship security zone*** is to operate around the ship while the ship is connected to the seabed beneath Australian waters. The ship security zone must be of a type prescribed under section 107.

47 After subsection 108(1)

Insert:

FPSOs and FSUs

(1A) In declaring under subsection 106(1AA) that a ship security zone is to operate around a security regulated ship, the Secretary must:

(a) have regard to the purpose of the zone; and

(b) take into account:

(i) the physical features of the ship; and

(ii) the operational features of the ship; and

(iii) the views of the ship operator for the ship; and

(c) if:

(i) it is likely that all or part of a security regulated offshore facility will be in the zone when the ship is connected to the seabed beneath Australian waters; and

(ii) the ship operator for the ship is not the offshore facility operator;

take into account the views of the offshore facility operator; and

(d) act consistently with Australia's obligations under international law.

48 After subsection 109(2)

Insert:

(2A) The regulations may provide that:

(a) if a ship security zone under subsection 106(1AA) comes into operation around a security regulated ship, the ship operator for the security regulated ship must, by writing, notify the coming into operation of the zone to each maritime industry participant (other than the ship operator for the security regulated ship) who conducts operations within the zone; and

(b) if the notice is given by the master of the security regulated ship, the notice is taken to have been given by the ship operator for the ship; and

(c) the notice must include prescribed information about the location and boundaries of the zone.

(2B) Subsection (2A) does not limit subsection (1).

49 Section 114 (paragraph beginning "Divisions 3 and 4")

Omit ", on board regulated Australian ships and on board ships regulated as offshore facilities", substitute "and on board regulated Australian ships".

50 Paragraph 122(1)(a)

Omit "or a ship regulated as an offshore facility".

51 Paragraph 123(a)

Omit "or a ship regulated as an offshore facility".

52 Paragraph 124(1)(a)

Omit ", on board a regulated Australian ship or on board a ship regulated as an offshore facility", substitute "or on board a regulated Australian ship".

53 Section 126

Omit ", on board a regulated Australian ship or on board a ship regulated as an offshore facility" (wherever occurring), substitute "or on board a regulated Australian ship".

54 Paragraph 129(1)(a)

Omit "or a ship regulated as an offshore facility".

55 Paragraph 130(a)

Omit "or a ship regulated as an offshore facility".

56 Paragraph 131(1)(a)

Omit ", on board a regulated Australian ship or on board a ship regulated as an offshore facility", substitute "or on board a regulated Australian ship".

57 Section 133

Omit ", on board a regulated Australian ship or on board a ship regulated as an offshore facility" (wherever occurring), substitute "or on board a regulated Australian ship".

58 Paragraph 138(1)(a)

Omit "or a ship regulated as an offshore facility".

59 Subsection 138(1) (note)

Omit "and 100Z(1) and (3)".

60 Paragraph 145A(2)(a)

Repeal the paragraph.

61 Paragraph 148A(2)(d)

Repeal the paragraph.

62 Section 150 (paragraph beginning "stop and search people")

Omit "and on ships regulated as offshore facilities".

63 Subsection 153(1)

Omit ", on a security regulated ship or on a ship regulated as an offshore facility", substitute "or on a security regulated ship".

64 Subsection 156(1)

Omit "or on a ship regulated as an offshore facility".

65 Subsection 163E(1)

Omit "or a ship regulated as an offshore facility".

66 Subsections 172(1), (4) and (5)

Omit "or a ship regulated as an offshore facility".

67 Subsection 178(1)

Omit "or a ship regulated as an offshore facility".

68 After paragraph 201(da)

Insert:

(db) to refuse to issue a certificate under section 89B or 89D; or

(dc) to cancel a certificate under section 89C or 89E; or

69 Paragraph 201(e)

Omit "or 100ZC".

70 Transitional—regulations made for the purposes of subsection 17(2) of the *Maritime Transport and Offshore Facilities Security Act 2003*

(1) This item applies to regulations made for the purposes of subsection 17(2) of the *Maritime Transport and Offshore Facilities Security Act 2003* that were in force immediately before the commencement of this item.

(2) The regulations have effect, after the commencement of this item, as if they were made for the purposes of subsection 17(2) of the *Maritime Transport and Offshore Facilities Security Act 2003* (as amended by this Schedule).

71 Transitional—FPSOs and FSUs

(1) This item applies if:

(a) an offshore security plan relates to a FPSO or a FSU; and

(b) the plan was in force immediately before the commencement of this item; and

(c) apart from this item, the FPSO or FSU is a regulated Australian ship.

(2) If a ship security plan comes into force in relation to the FPSO or FSU, the offshore security plan ceases to be in force.

(3) While the offshore security plan remains in force:

(a) the FPSO or FSU is taken to be:

(i) an offshore facility; and

(ii) a security regulated offshore facility;

for the purposes of the *Maritime Transport and Offshore Facilities Security Act 2003* (other than Divisions 4 and 5 of Part 4 of that Act); and

(b) the FPSO or FSU is taken not to be a regulated Australian ship for the purposes of the *Maritime Transport and Offshore Facilities Security Act 2003* (other than Divisions 4 and 5 of Part 4 of that Act).

Note 1: Divisions 4 and 5 of Part 4 of the *Maritime Transport and Offshore Facilities Security Act 2003* relate to security plans.

Note 2: This subitem means that approval for a ship security plan can be requested while the offshore security plan is still in force.

(4) For the purposes of the application of the *Maritime Transport and Offshore Facilities Security Act 2003* to the FPSO or FSU while the offshore security plan remains in force, disregard the amendments made by items 1, 8, 12, 14, 15, 17, 30, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 44, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67 and 69 of this Schedule.

Schedule 3—Amendments commencing day after Royal Assent

Part 1—Demerit points

Aviation Transport Security Act 2004

1 After subsection 44C(3)

Insert:

(3AA) To avoid doubt, regulations made for the purposes of subsection (1) may provide for the revocation of a person's approval as a known consignor, designation as a regulated air cargo agent or accreditation as an accredited air cargo agent, including in circumstances where the person has accumulated a specified number of demerit points.

Note: For the demerit points system, see Division 5 of Part 8.

2 Subsection 125(1)

Repeal the subsection, substitute:

(1) The regulations may establish a system (the ***demerit points system***) for and in relation to the following:

(a) the accrual of demerit points by aviation industry participants;

(b) the expiry of demerit points accrued by aviation industry participants;

(c) keeping a register of demerit points accrued by aviation industry participants.

Note: For the consequences of the demerit points system see sections 26 and 26G (about transport security programs) and subsection 44C(3AA) (about known consignors and regulated agents).

Part 2—Language modernisation

Aviation Transport Security Act 2004

3 Subsections 84(1A) and 89C(2)

Omit "sex", substitute "gender".

4 Subparagraph 95(5)(c)(i)

Omit "by a screening officer of the same sex as the person".

5 At the end of section 95

Add:

(6) A screening of a person in a private room as mentioned in paragraph (5)(c) must, if practicable, be conducted by a screening officer of the same gender as the person.

6 Subparagraph 95B(6)(c)(i)

Omit "by a screening officer of the same sex as the person".

7 At the end of section 95B

Add:

(7) A screening of a person in a private room as mentioned in paragraph (6)(c) must, if practicable, be conducted by a screening officer of the same gender as the person.

8 Paragraph 95C(6)(c)

Omit "by a screening officer of the same sex as the person".

9 At the end of section 95C

Add:

(7) A frisk search of a person in a private room as mentioned in paragraph (6)(c) must, if practicable, be conducted by a screening officer of the same gender as the person.

Maritime Transport and Offshore Facilities Security Act 2003

10 Section 145 (heading)

Omit "**, fax**".

11 Subsection 145(1)

Omit ", fax".

12 Section 145B (heading)

Omit "**, fax**".

13 Subsection 145B(1)

Omit ", fax".

14 Paragraph 166(5)(c)

Omit "by a screening officer of the same sex as the person".

15 At the end of section 166

Add:

(6) A screening of a person in a private room as mentioned in paragraph (5)(c) must, if practicable, be conducted by a screening officer of the same gender as the person.

16 Subparagraph 166B(6)(c)(i)

Omit "by a screening officer of the same sex as the person".

17 At the end of section 166B

Add:

(7) A screening of a person in a private room as mentioned in paragraph (6)(c) must, if practicable, be conducted by a screening officer of the same gender as the person.

18 Paragraph 166C(6)(c)

Omit "by a screening officer of the same sex as the person".

19 At the end of section 166C

Add:

(7) A frisk search of a person in a private room as mentioned in paragraph (6)(c) must, if practicable, be conducted by a screening officer of the same gender as the person.

20 Application of amendments

The amendments of sections 145 and 145B of the *Maritime Transport and Offshore Facilities Security Act 2003* made by this Part apply in relation to an application for a warrant made after the commencement of this item.

Part 3—Training requirements

Aviation Transport Security Act 2004

21 Paragraph 44C(1)(g)

After "training", insert ", qualification or other".

22 Subparagraph 44C(1)(g)(i)

Omit "or all regulated agents", substitute ", all regulated agents or all aircraft operators".

23 Subparagraphs 44C(1)(g)(ii) and (iii)

Omit "or regulated agents", substitute ", regulated agents or aircraft operators".

Part 4—Security directions

Aviation Transport Security Act 2004

24 After paragraph 67(1)(a)

Insert:

(aa) a general threat of unlawful interference with aviation is made or exists; or

25 Paragraph 67(1)(b)

After "the nature", insert ", or risk,".

25A After section 69

Insert:

69A Notification of special security directions

(1) The Secretary must, as soon as reasonably practicable after giving a special security direction, notify the Minister, in writing, of:
(a) the giving of the direction; and
(b) the terms of the direction.

(2) Failure to comply with this section does not affect the validity of the direction.

26 After subsection 70(4)

Insert:

(4A) The Secretary may, by writing, revoke a special security direction.

27 After subsection 70(5)

Insert:

(5A) A special security direction made under paragraph 67(1)(aa) must be revoked when the general threat no longer exists.

Maritime Transport and Offshore Facilities Security Act 2003

28 Subsection 33(1)

Repeal the subsection, substitute:

(1) If:

(a) a specific threat of unlawful interference with maritime transport or offshore facilities is made or exists; or

(b) a general threat of unlawful interference with maritime transport or offshore facilities is made or exists; or

(c) there is a change in the nature, or risk, of an existing general threat of unlawful interference with maritime transport or offshore facilities; or

(d) both of the following apply:

(i) a national emergency declaration (within the meaning of the *National Emergency Declaration Act 2020*) is in force;

(ii) the Secretary is satisfied that additional security measures are appropriate to support the national emergency declaration;

the Secretary may, in writing, direct that additional security measures be implemented or complied with.

29 Subsections 33(3) and (4)

Repeal the subsections.

29A Before section 37

Insert:

36B Notification of security directions

(1) The Secretary must, as soon as reasonably practicable after giving a security direction, notify the Minister, in writing, of:

(a) the giving of the direction; and

(b) the terms of the direction.

(2) Failure to comply with this section does not affect the validity of the direction.

30 Paragraph 37(3)(c)

Omit "33(3)(b)", substitute "33(1)(d)".

31 Subsection 38(1)

Repeal the subsection, substitute:

(1) The Secretary may, by writing, revoke a security direction.

(1A) A security direction covered by paragraph 33(1)(a) must be revoked when the specific threat no longer exists.

(1AA) A security direction covered by paragraph 33(1)(b) must be revoked when the general threat no longer exists.

32 Application of amendments

(1) The amendments of the *Aviation Transport Security Act 2004* made by this Part apply in relation to a special security direction given after the commencement of this item.

(2) The amendments of the *Maritime Transport and Offshore Facilities Security Act 2003* made by this Part apply in relation to a security direction given after the commencement of this item.

Part 5—Test weapons

Aviation Transport Security Act 2004

33 Section 9 (definition of *test weapon*)

Repeal the definition, substitute:

test weapon means:

(a) a weapon of a kind that is a replica or an imitation of another weapon; or

(b) a weapon that, as a result of a modification, is not capable of operating as a functional weapon; or

(c) a thing prescribed by the regulations to be a test weapon.

Part 6—Security regulated ports

Maritime Transport and Offshore Facilities Security Act 2003

34 Section 10 (definition of *port facility*)

Repeal the definition, substitute:

port facility means an area of land or water, or land and water, within a security regulated port (including any buildings, installations or equipment in or on the area) used either wholly or partly in connection with one or more of the following:

(a) the movement, loading, unloading, maintenance or provisioning of security regulated ships;

(b) the movement of goods that have been, or are intended to be, transported by security regulated ship;

(c) the storage of goods that have been, or are intended to be, transported by security regulated ship;

(d) the loading of goods that have been transported by security regulated ship on to another mode of transport;

(e) the unloading of goods that are intended to be transported by security regulated ship from another mode of transport;

(f) any other activity or thing that is critical to ensuring the security and reliability of an activity mentioned in any of the above paragraphs.

35 Subsection 12(1)

Repeal the subsection, substitute:

(1) A ***port*** is one or more areas of land or water, or land and water, (including any buildings, installations or equipment situated in or on the land or water, or land and water) intended for use either wholly or partly in connection with one or more of the following:

(a) the movement, loading, unloading, maintenance or provisioning of ships;

(b) the movement of goods that have been, or are intended to be, transported by ship;

(c) the storage of goods that have been, or are intended to be, transported by ship;
(d) the loading of goods that have been transported by ship on to another mode of transport;
(e) the unloading of goods that are intended to be transported by ship from another mode of transport;
(f) any other activity or thing that is critical to ensuring the security and reliability of an activity mentioned in any of the above paragraphs.

36 Subsection 13(1)

Repeal the subsection, substitute:

(1) The Secretary may, by notice published in the Gazette, declare that areas of a port comprise a ***security regulated port*** if the areas are intended for use either wholly or partly in connection with one or more of the following:
(a) the movement, loading, unloading, maintenance or provisioning of security regulated ships;
(b) the movement of goods that have been, or are intended to be, transported by security regulated ship;
(c) the storage of goods that have been, or are intended to be, transported by security regulated ship;
(d) the loading of goods that have been transported by security regulated ship on to another mode of transport;
(e) the unloading of goods that are intended to be transported by security regulated ship from another mode of transport;
(f) any other activity or thing that is critical to ensuring the security and reliability of an activity mentioned in any of the above paragraphs.

37 Transitional—security regulated ports

A notice:
(a) published under subsection 13(1) of the *Maritime Transport and Offshore Facilities Security Act 2003*, as in force before the commencement of this Part; and
(b) that is in force immediately before that commencement;

continues in force (and may be dealt with) at and after that commencement as if the notice were published under subsection 13(1) of the *Maritime Transport and Offshore Facilities Security Act 2003*, as substituted by this Part.

38 Transitional—port facility operators

(1) This item applies if:

(a) immediately before the commencement of this item, a person was not a port facility operator in relation to an area within a security regulated port; and

(b) at that commencement, the person is a port facility operator in relation to the area.

Note: This item covers persons who, at the commencement of this item, become port facility operators in relation to areas within a security regulated port as a result of the substitution of the definition of ***port facility*** in section 10 of the *Maritime Transport and Offshore Facilities Security Act 2003* made by this Part.

(2) Sections 42 and 43 of the *Maritime Transport and Offshore Facilities Security Act 2003* do not apply to the person, for the period referred to in subitem (3), to the extent that those sections would (apart from this item) apply to the person as a port facility operator in relation to the area.

(3) The period is the period starting at the commencement of this item and ending at the earlier of the following times:

(a) at the time a notice that covers all or part of the area is first published, under subsection 13(1) of the *Maritime Transport and Offshore Facilities Security Act 2003*, after the commencement of this item;

(b) at the time a maritime security plan for the person as a port facility operator in relation to the area first comes into force, under Division 5 of Part 3 of that Act, after the commencement of this item.

Part 7—Increased penalties

Aviation Transport Security Act 2004

39 Subsections 13(1) and 14(1) (penalty)

Omit "200 penalty units", substitute "300 penalty units".

40 Paragraphs 35(3)(a), 36(3)(a), 36A(3)(a), 37(3)(a), 38(3)(a) and 38A(3)(a)

Repeal the paragraphs, substitute:

(a) for an offence committed by an airport operator, an aircraft operator or a screening authority—250 penalty units; or

41 Paragraph 38AB(3)(a)

Omit "200 penalty units", substitute "250 penalty units".

42 Subsection 38B(1)

Omit "50 penalty units", substitute "250 penalty units".

43 At the end of subsection 38B(1)

Add:

Note: If a body corporate is convicted of an offence against regulations made for the purposes of this section, subsection 4B(3) of the *Crimes Act 1914* allows a court to impose fines of up to 5 times the penalty stated in this subsection.

44 Paragraph 44(4)(a)

Repeal the paragraph, substitute:

(a) for an offence committed by an airport operator, an aircraft operator or a screening authority—250 penalty units; or

45 Paragraphs 44C(4)(a), 52(3)(a), 60(3)(a), 62(2)(a) and 65(3)(a)

Omit "200 penalty units", substitute "250 penalty units".

46 Subsections 65C(1), 73(1) and 74C(1) (penalty)

Omit "200 penalty units", substitute "300 penalty units".

47 Subsection 74K(3)

Omit "50 penalty units", substitute "250 penalty units".

48 At the end of section 74K

Add:

Note: If a body corporate is convicted of an offence against regulations made for the purposes of this section, subsection 4B(3) of the *Crimes Act 1914* allows a court to impose fines of up to 5 times the penalty stated in this subsection.

49 Subsections 100(1) and 101(1) (penalty)

Omit "200 penalty units", substitute "300 penalty units".

50 Paragraph 133(2)(b)

Omit "50 penalty units", substitute "250 penalty units".

51 At the end of subsection 133(2)

Add:

Note: If a body corporate is convicted of an offence against regulations made under this section, subsection 4B(3) of the *Crimes Act 1914* allows a court to impose fines of up to 5 times the penalty stated in paragraph (b).

52 Subsection 133(3)

Omit "50 penalty units", substitute "250 penalty units".

53 Transitional provision

The amendments of sections 35, 36, 36A, 37, 38, 38A, 38AB, 38B, 44, 44C, 52, 60, 62, 65, 74K and 133 of the *Aviation Transport Security Act 2004* made by this this Part do not affect the validity of regulations in force for the purposes of those provisions immediately before the commencement of this item.

[*Minister's second reading speech made in—*
House of Representatives on 28 November 2024
Senate on 25 March 2025]

(166/24)