Maritime Transport and Offshore Facilities Security Regulations 2003

Statutory Rules No. 366, 2003

made under the

Maritime Transport and Offshore Facilities Security Act 2003

Compilation No. 42

Compilation date:	23 August 2021
Includes amendments up to:	F2021L01145
Registered:	9 September 2021

Prepared by the Office of Parliamentary Counsel, Canberra

Replaced Authorised Version registered 19/04/2024 F2021C00921

About this compilation

This compilation

This is a compilation of the *Maritime Transport and Offshore Facilities Security Regulations 2003* that shows the text of the law as amended and in force on 23 August 2021 (the ***compilation date***).

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

Uncommenced amendments

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

Application, saving and transitional provisions for provisions and amendments

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

Editorial changes

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

Modifications

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

Self-repealing provisions

If a provision of the compiled law has been repealed in accordance with a provision of the law, details are included in the endnotes.

Contents

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 1—Preliminary

1.01 Name of Regulations

These Regulations are the *Maritime Transport and Offshore Facilities Security Regulations 2003*.

1.03 Interpretation

(1) In these Regulations:

ABN (short for Australian Business Number) has the meaning given by section 41 of the *A New Tax System (Australian Business Number) Act 1999*.

ACN (short for Australian Company Number) has the meaning given by section 9 of the *Corporations Act 2001*.

Act means the *Maritime Transport and Offshore Facilities Security Act 2003*.

airport has the meaning given by the *Aviation Transport Security Act 2004*.

ARBN (short for Australian Registered Body Number) has the meaning given by section 9 of the *Corporations Act 2001*.

Australian Federal Police employee has the same meaning as AFP employee in subsection 4(1) of the *Australian Federal Police Act 1979*.

cleared zone means a type of port security zone, established by the Secretary under subsection 102(1) of the Act, that comprises an area of land or water, to which access is controlled, for holding persons and goods, vehicles or vessels that have been screened and cleared.

contact details, for a person, includes:

(a) the person's business address, mailing address, fixed-line telephone number, mobile telephone number and e-mail address; and

(b) if the person is a CSO, SSO, PSO or PFSO—a single 24-hour fixed-line or mobile telephone number for the person; and

(c) if the person is an OFSO or OSPSO—a single 24-hour fixed-line and a mobile telephone number for the person.

contracting government means a contracting government to the SOLAS Convention.

Note: For the definition of ***SOLAS Convention***, see section 10 of the Act.

CSO or ***company security officer*** has the meaning given by regulation 1.10.

exclusion zone means a ship security zone, declared by the Secretary to operate under subsection 106(1) or (1A) of the Act, that comprises an area of water, at and below the water level:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(a) within a security regulated port, being an area to which access is controlled and that surrounds a security regulated ship; or

(b) in the vicinity of a security regulated offshore facility, being an area to which access is controlled and that surrounds a security regulated ship which is engaged in any activity in relation to the facility.

HSO or ***head security officer*** has the meaning given by regulation 1.32.

IMO means the International Maritime Organization.

inter-State voyage, in relation to a ship, means a voyage (other than an overseas voyage) in the course of which the ship travels between:

(a) a port in a State and a port in another State; or

(b) a port in a State and a port in a Territory; or

(c) a port in a Territory and a port in another Territory;

whether or not the ship travels between 2 or more ports in any one State or Territory in the course of the voyage.

land-side restricted zone means a type of port security zone, established by the Secretary under subsection 102(1) of the Act, that comprises an area of land or a structure connected directly or indirectly to land, to which access is controlled, within the boundaries of a port facility or of land under the control of a port operator.

large passenger ship means either of the following:

(a) a regulated Australian ship of a kind mentioned in paragraph 16(1)(a) of the Act that has a maximum capacity of 151 or more passengers;

(b) a regulated foreign ship of a kind mentioned in subparagraph 17(1)(b)(i) of the Act that has a maximum capacity of 151 or more passengers.

maritime security outcome means an outcome set out in subsection 3(4) of the Act.

member of the Australian Federal Police has the same meaning as in subsection 4(1) of the *Australian Federal Police Act 1979*.

official number, for a ship, means the number by which the ship is identified in the Australian Register of Ships mentioned in section 56 of the *Shipping Registration Act 1981*.

offshore facility zone means a type of offshore security zone, established by the Secretary under subsection 113A(1) of the Act, that comprises the space occupied by an offshore facility.

offshore service provider means a person prescribed by regulation 1.06.

offshore water-side zone means a type of offshore security zone established by the Secretary under subsection 113A(1) of the Act, that comprises an area of water surrounding an offshore facility at the distance from the facility specified by the Secretary.

Replaced Authorised Version registered 19/04/2024 F2021C00921

OFSO or ***offshore facility security officer*** has the meaning given by regulation 1.33.

on-board restricted area means an on-board security zone, established by the Secretary under subsection 110(1) of the Act, that comprises an area, to which access is controlled, on board a regulated Australian ship.

OSPSO or ***offshore service provider security officer*** has the meaning given by regulation 1.34.

parent: without limiting who is a parent of anyone for the purposes of these Regulations, a person is the ***parent*** of another person if the other person is a child of the person within the meaning of the *Family Law Act 1975*.

PFSO or ***port facility security officer*** has the meaning given by regulation 1.25.

pleasure craft means a ship that is used, or intended to be used, wholly for recreational or sporting activities.

pre-entry information has the meaning given by subregulation 4.80(2).

PSO or ***port security officer*** has the meaning given by regulation 1.20.

RFSSO or ***regulated foreign ship security officer*** means:

(a) the master of a regulated foreign ship; or

(b) an officer on board a regulated foreign ship who is accountable to the master of the ship for:

(i) ensuring that the ship complies with section 97 of the Act; and

(ii) liaising with company, ship, port and port facility security officers before the ship enters, or while the ship is in, a security regulated port.

security barrier has the meaning given by regulation 6.25.

security plan audit means an audit relating to one or more of the following plans to determine if security measures and procedures set out in the plan have been implemented and complied with:

(a) a maritime security plan;

(b) a ship security plan;

(c) an offshore security plan.

security plan review means a review of one or more of the following plans to determine if security measures and procedures set out in the plan are effective and adequate:

(a) a maritime security plan;

(b) a ship security plan;

(c) an offshore security plan.

ship/facility interface means the interaction that occurs when a ship interacts with an offshore facility so that the facility is directly and immediately affected by activities involving the movement of persons or goods.

Replaced Authorised Version registered 19/04/2024 F2021C00921

ship/port interface means the interaction that occurs when a security regulated ship is directly and immediately affected by activities involving:

(a) the movement of persons or goods; or

(b) the provision of port services to or from the ship.

shore-based personnel, in relation to a regulated Australian ship, means the body of persons (other than crew) employed by the ship operator for the ship.

small passenger ship means either of the following:

(a) a regulated Australian ship of a kind mentioned in paragraph 16(1)(a) of the Act that has a maximum capacity of more than 12 passengers but not more than 150 passengers;

(b) a regulated foreign ship of a kind mentioned in subparagraph 17(1)(b)(i) of the Act that has a maximum capacity of more than 12 passengers but not more than 150 passengers.

SSO or ***ship security officer*** has the meaning given by regulation 1.15.

supply base means a place, at a port or airport, where goods or passengers are loaded on to a vessel or aircraft for transport directly from the place to an offshore facility.

water-side restricted zone has the meaning given by regulation 1.70.

working day, in relation to the operations of a maritime industry participant, means a day other than a Saturday, a Sunday, or a day that is a public holiday in the State or Territory where the operations are conducted.

(2) An expression used in these Regulations and in the ISPS Code has in these Regulations the same meaning as in the ISPS Code, unless the contrary intention appears.

1.04 Purposes of these Regulations

The purposes of these Regulations are:

(a) to ensure that maritime, ship and offshore security plans address specific matters that will satisfy the Secretary that the implementation of the plans will make an appropriate contribution towards the achievement of the maritime security outcomes; and

(b) to set out the requirements for maritime, ship and offshore security plans (including matters that must be dealt with in the plans) so that:

(i) persons preparing maritime, ship and offshore security plans know what they need to do for the plans to receive approval; and

(ii) plans are consistent in terms of layout and general content; and

(iii) the criteria for approval of plans are clear; and

(c) to prescribe matters that are required, permitted, necessary or convenient to be prescribed, including:

(i) requirements in relation to the giving of security and control directions; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(ii) types of port, ship, on-board and offshore security zones; and
(iii) requirements in relation to screening and clearing; and
(iv) kinds of weapons and prohibited items.

1.05 Operators prescribed as maritime industry participants

(1) For paragraph (g) of the definition of ***maritime industry participant*** in section 10 of the Act, an operator of a kind set out in subregulation (2) is prescribed if the operator provides port services to security regulated ships.

(2) For subregulation (1), the following are the kinds of operators:
(a) lighter operator;
(b) barge operator;
(c) line handling boat operator;
(d) pilotage service operator;
(e) tug operator.

1.06 Offshore service providers (Act s 10)

For paragraph (c) of the definition of ***offshore industry participant*** in section 10 of the Act, a person that manages a supply base is prescribed.

1.10 Company security officers

(1) Before requesting the Secretary to approve a ship security plan, the ship operator for a regulated Australian ship must designate, in writing, a person within the ship operator's organisation as security officer (***company security officer*** or ***CSO***) for the ship.

(2) A CSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of a CSO include:
(a) answering any questions about the ship security plan, and acting as contact officer, during the approval process; and
(b) implementing and maintaining the ship security plan for the ship; and
(c) liaising with the SSO for the ship and with port and port facility security officers; and
(d) performing:
(i) the duties and responsibilities in section 11.2 of Part A of the ISPS Code; and
(ii) any additional duties and responsibilities set out in the ship security plan.

(4) The ship operator must ensure that a CSO:
(a) has the knowledge and ability to perform the duties of a CSO; and
(b) is given the training set out in the ship security plan; and
(c) is a suitable person to access and handle security information; and
(d) has the authority to act on instructions received from the Secretary.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Example: A CSO must have the authority to implement security directions or a change in the security level.

1.15 Ship security officers

(1) The ship operator for a regulated Australian ship must designate, in writing, the master, or another crew member, of the ship as security officer (***ship security officer*** or ***SSO***).

(2) An SSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of an SSO include:
  (a) maintaining the ship security plan for the ship; and
  (b) liaising with the CSO for the ship and with ship, port and port facility security officers; and
  (c) performing:
    (i) the duties and responsibilities in section 12.2 of Part A of the ISPS Code; and
    (ii) any additional duties and responsibilities set out in the ship security plan.

(4) The ship operator must ensure that an SSO:
  (a) holds a certificate of proficiency as a ship security officer:
    (i) issued under the Marine Orders, Part 3 (Seagoing Qualifications); and
    (ii) that is valid within the meaning of that Part; and
  (b) is given the training set out in the ship security plan; and
  (c) is a suitable person to access and handle security information; and
  (d) has the authority to act on instructions received from the Secretary or ship operator.

Example: An SSO must have the authority to implement security directions or a change in the security level.

(5) An SSO who is not the master of the ship is accountable to the master of the ship.

1.20 Port security officers

(1) Before requesting the Secretary to approve a maritime security plan, a port operator for a security regulated port must designate, in writing, a person as security officer (***port security officer*** or ***PSO***).

(2) A PSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of a PSO include:
  (a) conducting an initial security survey of the port and facilitating the completion of the security assessment for the port operator's maritime security plan; and
  (b) ensuring the development and maintenance of the maritime security plan for the port operator; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(c) implementing the maritime security plan; and
(d) undertaking regular security inspections of the port to ensure the effectiveness and adequacy of security measures; and
(e) facilitating security plan reviews; and
(f) recommending and incorporating modifications to the maritime security plan in order to:
(i) correct deficiencies in the plan; or
(ii) update the plan to take into account changes to the port; and
(g) enhancing security awareness and vigilance of port personnel; and
(ga) without limiting paragraph (g), ensuring that port personnel are provided with adequate training in security awareness; and
(h) ensuring that standards for personnel with, or who have been assigned, security duties and responsibilities are met and that adequate training is provided to such personnel; and
(i) reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the port; and
(j) liaising with ship and port facility security officers; and
(k) coordinating with security, police, fire, ambulance, medical, search and rescue services, as appropriate; and
(l) ensuring that security equipment is properly operated, inspected, tested, calibrated and maintained; and
(m) when requested by an SSO, assisting in confirming the identity of persons intending to board a ship; and
(n) providing advice to the Secretary on the operational and safety aspects of the implementation of security and control directions; and
(o) communicating and coordinating the implementation of security and control directions.

(4) A port operator must ensure that a PSO:
(a) has the knowledge and ability to perform the duties of a PSO; and
(b) is given the training set out in the maritime security plan for the port operator; and
(c) is a suitable person to access and handle security information; and
(d) has the authority to act on instructions received from the Secretary.

1.25 Port facility security officers

(1) Before requesting the Secretary to approve a maritime security plan, a port facility operator must designate, in writing, a person as security officer (***port facility security officer*** or ***PFSO***) for the port facility.

(2) A PFSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of a PFSO include:
(a) facilitating the development, implementation, revision and maintenance of the maritime security plan for the port facility operator; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(b) liaising with ship, company, port and other port facility security officers; and

(ba) ensuring that port facility personnel are provided with adequate training in security awareness; and

(c) performing:

(i) the duties and responsibilities in section 17.2 of Part A of the ISPS Code; and

(ii) any additional duties and responsibilities set out in the maritime security plan.

(4) A port facility operator must ensure that a PFSO:

(a) has the knowledge and ability to perform the duties of a PFSO; and

(b) is given the training set out in the maritime security plan for the port facility operator; and

(c) is a suitable person to access and handle security information; and

(d) has the authority to act on instructions received from the Secretary.

1.32 Head security officer

(1) Before requesting the Secretary to approve an offshore security plan, an offshore facility operator must designate, in writing, a person within the operator's organisation as a security officer (a ***head security officer*** or ***HSO***) for all the operator's facilities.

(2) An HSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of an HSO include:

(a) answering any questions about the plan, and acting as contact officer, during the approval process; and

(b) implementing and maintaining the plan for the facility or facilities; and

(c) liaising with the OFSO for each facility and with OSPSOs; and

(d) performing any additional duties and responsibilities set out in the plan.

(4) The offshore facility operator must ensure that an HSO:

(a) has the knowledge and ability to perform the duties of an HSO; and

(b) is given the training set out in the plan; and

(c) is a suitable person to access and handle security information; and

(d) has the authority to act on instructions received from the Secretary; and

(e) is located in Australia at a place that is not an offshore facility.

Example: For paragraph (4)(d), an HSO must have the authority to implement security directions or a change in the security level.

1.33 Offshore facility security officers

(1) Before requesting the Secretary to approve an offshore security plan for an offshore facility, an offshore facility operator must designate, in writing, a person as security officer (an ***OFSO*** or ***offshore facility security officer***) for the facility.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) An OFSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of an OFSO include:

(a) conducting an initial security survey of the facility and facilitating the completion of the security assessment for the security plan; and

(b) ensuring the development and maintenance of the security plan; and

(c) implementing the security plan; and

(d) undertaking regular security inspections of the facility to ensure the effectiveness and adequacy of security measures; and

(e) facilitating security plan reviews; and

(f) recommending and incorporating modifications to the security plan in order to:

(i) correct deficiencies in the plan; or

(ii) update the plan to take into account changes to the facility; and

(g) enhancing security awareness and vigilance of facility personnel; and

(h) ensuring that standards for personnel with, or who have been assigned, security duties and responsibilities are met and that adequate training is provided to the personnel; and

(i) reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the facility; and

(j) liaising with ship security officers and offshore industry participants' security officers; and

(k) coordinating with security, police, fire, ambulance, medical, search and rescue services, as appropriate; and

(l) ensuring that security equipment is properly operated, inspected, tested, calibrated and maintained; and

(m) confirming the identity of persons intending to enter the facility; and

(n) providing advice to the Secretary on the operational and safety aspects of the implementation of security and control directions; and

(o) communicating and coordinating the implementation of security and control directions.

(4) A facility operator must ensure that an OFSO:

(a) has the knowledge and ability to perform the duties of an OFSO; and

(b) is given the training set out in the offshore security plan for the facility operator; and

(c) is a suitable person to access and handle security information; and

(d) has the authority to act on instructions received from the Secretary.

1.34 Offshore service provider security officers

(1) Before requesting the Secretary to approve an offshore security plan, an offshore service provider must designate, in writing, a person as security officer (an ***offshore service provider security officer*** or ***OSPSO***) for the service.

(2) An OSPSO may be designated by name or by reference to a position.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(3) The duties and responsibilities of an OSPSO include:

(a) conducting an initial security survey of the activities of the service provider and facilitating the completion of the security assessment for the security plan; and

(b) ensuring the development and maintenance of the security plan; and

(c) implementing the security plan; and

(d) undertaking regular security inspections of the service provider's supply base to ensure that the security measures are adequate and as effective as possible; and

(e) facilitating security plan reviews; and

(f) recommending and incorporating modifications to the security plan in order to:

(i) correct deficiencies in the plan; or

(ii) update the plan to take into account changes to the facility; and

(g) enhancing security awareness and vigilance of the service provider's personnel; and

(h) ensuring that standards for personnel with, or who have been assigned, security duties and responsibilities are met and that adequate training is provided to the personnel; and

(i) reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the service provider; and

(j) liaising with the security officers of ships and offshore industry participants; and

(k) coordinating with security, police, fire, ambulance, medical, search and rescue services, as appropriate; and

(l) ensuring that security equipment is properly operated, inspected, tested, calibrated and maintained; and

(m) when requested by an OFSO, assisting in confirming the identity of persons intending to enter an offshore facility; and

(n) providing advice to the Secretary on the operational and safety aspects of the implementation of security and control directions; and

(o) communicating and coordinating the implementation of security and control directions.

(4) A service provider must ensure that an OSPSO:

(a) has the knowledge and ability to perform the duties of an OSPSO; and

(b) is given the training set out in the security plan for the service provider; and

(c) is a suitable person to access and handle security information; and

(d) has the authority to act on instructions received from the Secretary.

1.35 Delegation by security officers

(1) A CSO, SSO, PSO, PFSO, HSO, OFSO or OSPSO may delegate, in writing, some or all of his or her powers (except this power of delegation), functions and duties.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) A delegation under this regulation:

(a) may only be made to a person who has the knowledge and ability to exercise or perform the powers, functions or duties to be delegated; and

(b) must specify the delegate by name.

1.40 Shore-based personnel and crew

The ship operator for a regulated Australian ship must ensure that shore-based personnel and crew identified in the ship security plan as having security duties and responsibilities:

(a) have the knowledge and ability to perform their security-related duties and responsibilities; and

(b) are given the training set out in the plan.

1.45 Declarations of security

(1) A declaration of security involving a ship and another party must be signed and dated by the master of, or SSO for, the ship and:

(a) if the other party to the agreement is also a ship—the master of, or SSO for, that other ship; or

(b) if the other party to the agreement is a port operator—the PSO; or

(c) if the other party to the agreement is a port facility operator—the PFSO.

(1A) A declaration of security involving an offshore facility and another party must be signed and dated by the operator of, or HSO for, the facility and:

(a) if the other party to the agreement is a ship—the master of, or SSO for, the ship; or

(b) if the other party to the agreement is an offshore industry participant that operates an offshore service—the security officer for the participant.

(2) A declaration of security must set out:

(a) contact details for the parties and signatories to the agreement; and

(b) the period for which the declaration is valid; and

(c) the maritime security level in force for each party.

Note: A sample form of a declaration of security is available on the Department's web site—see http://www.infrastructure.gov.au.

(3) A copy of the declaration of security must be kept by a party to the agreement for a period of 7 years beginning on the day after the declaration ceases to be valid.

1.50 Security plan audits and reviews

(1) A security plan audit or review must be conducted in accordance with the schedule, requirements and procedures set out in the maritime, ship or offshore security plan.

(2) A security plan review must be conducted as soon as practicable after a maritime transport or offshore facility security incident.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(3) The records of each security plan audit or review must be kept for a period of 7 years beginning on the day after the audit or review is concluded.

1.55 Ship security records—regulated Australian ships

(1) A regulated Australian ship must keep a record of the following information in relation to the ship:

(a) unless paragraph (aa) applies—the approved ship security plan for the ship;

(aa) if the Secretary has, in accordance with section 61A of the Act, granted the ship operator an exemption from the operation of Division 2 of Part 4 of the Act—a copy of the exemption;

(b) whether the ship possesses a valid ISSC;

(ba) if the Secretary has, in accordance with section 79A of the Act, granted the ship operator an exemption from the operation of Division 6 of Part 4 of the Act—a copy of the exemption;

(c) the period of validity, and the name of the issuing authority, of the ISSCs possessed by the ship;

(d) the security level at which the ship is operating;

(e) the security levels at which the ship operated at ports and offshore facilities, and specific periods during which the ship operated at those levels, while conducting ship/port interfaces and ship/facility interfaces;

(f) any special or additional security measures that were implemented by the ship in any port or offshore facility where it conducted ship/port interface or ship/facility interface;

(g) whether appropriate ship security procedures were maintained during any ship to ship activity;

(h) if ship security procedures referred to in paragraph (g) were maintained—the procedures and the specific periods during which those procedures were maintained;

(i) training, drills and exercises;

(j) security threats and maritime transport security incidents;

(k) breaches of security;

(l) changes to security levels;

(m) communications relating to the direct security of the ship (such as specific threats to the ship or to port or offshore facilities used in connection with the loading or unloading of the ship);

(n) ship security plan audits and reviews;

(o) periodic review of ship security assessments;

(p) periodic ship security plan reviews;

(q) implementation of any amendments to the ship security plan;

(r) inspection, testing, calibration and maintenance of security equipment (including ship security alert system);

(s) other practical security-related information in accordance with regulation XI-2/9.2.1 of the SOLAS Convention.

Note: For the definition of ***SOLAS Convention***, see section 10 of the Act.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) For the definition of ***ship security record*** in section 10 of the Act, the following are prescribed to be kept on, by and for a regulated Australian ship:

(a) a document made for the purposes of keeping records required under subregulation (1);

(b) any information included in such a document.

(3) Ship security records must be made available for inspection in accordance with the Act and these Regulations.

(3A) Ship security records in relation to the following matters must be made available for inspection at the request of a person who is authorised by a contracting government to inspect the records:

(a) the security level at which the ship is operating;

(b) the security level at which the ship operated in the last 10 ports of call where it conducted ship/port interface or ship/facility interface;

(c) any special or additional security measures that were implemented by the ship in the last 10 ports of call;

(d) any ship security procedures maintained by the ship in the last 10 ports of call where it conducted ship to ship activities;

(e) the name of the person responsible for appointing:

(i) the ship's crew; and

(ii) other persons employed or engaged in any capacity on board the ship and on the business of the ship;

(f) the name of the person who decides how the ship is to be employed;

(g) if the ship is employed under the terms of a charter party or of charter parties, the names of the parties to the charter arrangements;

(h) other practical security-related information (except details of the ship security plan for the ship) in accordance with regulation XI-2/9.2.1 of the SOLAS Convention.

Note 1: For the definition of ***SOLAS Convention***, see section 10 of the Act.

Note 2: For provisions that identify who may inspect the ISSC for a regulated Australian ship, see regulation 4.145 and subparagraphs 139(2)(e)(i) and 148(2)(c)(i) of the Act.

(4) Ship security records must be kept on board the ship for a period of 7 years beginning on:

(a) in the case of a document—the date of the document or, if the document consists of a series of entries, the date when the latest entry is made on the document; or

(b) in the case of information—the date when the information was obtained or, if the information is part of a document that consists of a series of entries, the date when the latest entry is made on the document.

1.56 Ship security records—regulated foreign ships

For the definition of ***ship security record*** in section 10 of the Act, the following are prescribed to be kept on, by and for a regulated foreign ship:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(a) confirmation that a valid ISSC, or approved ISSC equivalent under subsection 91(3) of the Act, is on board the ship;
(b) the name of the authority that issued the ship's ISSC or approved ISSC equivalent;
(c) the date when the ISSC or approved ISSC equivalent expires;
(d) any document made for the purpose of keeping records in relation to:
  (i) the security level at which the ship is operating; and
  (ii) the security level at which the ship operated in the last 10 ports of call where the ship conducted ship/port interface or ship/facility interface; and
  (iii) whether the ship implemented any special or additional security measures in the last 10 ports of call; and
  (iv) whether appropriate security-related procedures were maintained in the last 10 ports of call where the ship conducted ship to ship activities;
(e) the name of the person responsible for appointing:
  (i) the ship's crew; and
  (ii) other persons employed or engaged in any capacity on board the ship and on the business of the ship;
(f) the name of the person who decides how the ship is to be employed;
(g) if the ship is employed under the terms of a charter party or of charter parties—the names of the parties to the charter arrangements;
(h) other practical security-related information (except details of the ship security plan for the ship) in accordance with regulation XI-2/9.2.1 of the SOLAS Convention.

Note: For the definition of ***SOLAS Convention***, see section 10 of the Act.

1.60 Prohibited items

For the definition of ***prohibited item*** in section 10 of the Act, the following are prescribed:

(a) an imitation or replica of a firearm;
(b) an imitation or replica of a bomb, grenade, rocket, missile or mine.

1.65 Weapon

(1) For the definition of ***weapon*** in section 10 of the Act, a thing set out or described in column 2 of an item in table 1.65 is a weapon.

(2) Despite anything in table 1.65, a flare or other incendiary safety device is not a weapon if it is carried on board a ship or is kept on an offshore facility as part of the ship's, or facility's, safety or signalling equipment.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Table 1.65 Weapons

Item	Things or description of things
1	Bombs and grenades
2	Live rockets or missiles
3	Things, other than those included in items 1 and 2: (a) that are, or in the nature of, explosives or incendiary devices; or (b) that contain or expel gas or other irritants (such as tear gas canisters and smoke cartridges), whether or not live
4	Flame throwers that are of military design, or other devices that are capable of projecting ignited incendiary fuel
5	Crossbows or other similar devices consisting of a bow fitted transversely on a stock that has a groove or barrel designed to direct an arrow or bolt
6	Electromagnetic weapons, or other devices made or modified to emit electromagnetic radiation so as to injure or disable a person
7	Acoustic or light emitting anti personnel devices
8	Rocket launchers, recoilless rifles, antitank rifles, bazookas or rocket-propelled-grenade-type launchers

1.70 Water-side restricted zone

(1) A port security zone, established by the Secretary under subsection 102(1) of the Act, that comprises an area of water within a security regulated port is a ***water-side restricted zone*** if:

(a) the area is one where a security regulated ship may berth, anchor or moor; and

(b) access to the area is controlled.

(2) A water-side restricted zone extends below the water level to the seabed and under any wharf adjacent to the zone.

1.72 Prescribed kinds of regulated Australian ships

For paragraph 16(1)(d) of the Act, an Australian ship that:

(a) is capable of being used to carry both passengers and vehicles on inter-State voyages; and

(b) is used to carry both passengers and vehicles on inter-State voyages;

is prescribed.

1.75 What are not regulated Australian ships

For subsection 16(2) of the Act, a passenger ship (whether or not also a cargo ship) used for overseas voyages is not a regulated Australian ship if the ship is a pleasure craft that is not engaged in trade.

Replaced Authorised Version registered 19/04/2024 F2021C00921

1.80 What are not regulated foreign ships

For subsection 17(2) of the Act, a foreign ship that meets the requirements of paragraphs 17(1)(b) to (d) of the Act is not a regulated foreign ship if:

(a) the ship is owned or operated by a contracting government and is used, for the time being, only on government non-commercial service; or

(b) the ship is a pleasure craft that is not engaged in trade.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 2—Maritime security levels and security directions

Division 2.1—Preliminary

Note: This Division heading is reserved for future use.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 2.2—Maritime security levels

2.25 Notifying maritime security level 2 and 3 declarations and revocations (Act s 32)

(1) This regulation applies to notifying declarations, or revocations of declarations, under Division 3 of Part 2 of the Act.

(2) The Secretary or port operator must notify a declaration or revocation:
  (a) orally (for example, by telephone or radio communication); or
  (b) in writing; or
  (c) by electronic transmission (for example, by fax or e-mail).

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 2.3—Security directions

2.30 Requirement for consultation

If it is reasonable and practicable to do so, the Secretary must consult with the following about giving a security direction that relates to the movement of ships within, or in or out of, a security regulated port or in an offshore water-side zone:

(a) maritime industry or offshore industry participants who will be affected by the direction;

(b) agencies of the Commonwealth, a State or Territory whose operations in the port will be affected by the direction;

(c) persons, other than those mentioned in paragraph (a) or (b), who need to implement, or comply with, the direction.

Examples: For paragraph (c), harbour masters and PSOs.

2.35 Giving and communicating security directions (Act s 33(5))

(1) Subject to subsections 35(2) and 38(3) of the Act, the Secretary must give a security direction, or notify a person of the revocation of a security direction under subsection 38(2) of the Act:

(a) orally (for example, by telephone or radio communication); or

(b) in writing; or

(c) by electronic transmission (for example, by fax or e-mail).

Note: Under subsection 33(4) of the Act, a security direction has no effect until the Secretary commits the direction to writing.

(2) Each of the following:

(a) a port operator required to communicate a security direction under subsection 35(3) of the Act;

(b) an offshore facility operator required to communicate a security direction under subsection 35(8) of the Act;

(c) a ship operator required to communicate a security direction under subsection 36(2) of the Act;

must do so using any of the means set out in subregulation (1).

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 3—Maritime security plans

Division 3.1—Preliminary

3.05 Common requirements for security assessments

A security assessment for a maritime security plan must include the following matters:

(a) the date when the assessment was completed or reviewed;

(b) the scope of the assessment, including assets, infrastructure and operations assessed;

(c) a summary of how the assessment was conducted, including details of the risk management process adopted;

(d) the skills and experience of the key persons who completed or participated in the assessment.

3.10 Common requirements for security plan audits and reviews

A maritime security plan for a port operator or port facility operator must set out:

(a) a schedule of security plan audits; and

(b) the circumstances, in addition to the occurrence of a maritime transport security incident, following which a security plan review must be conducted; and

(c) the procedures for conducting a security plan audit, including a process for selecting auditors who are independent of the matters being audited; and

(d) the procedures for conducting a security plan review, including a process for consultation during the review.

3.11 Common requirements for maps included with maritime security plans

(1) A map mentioned in sections 49 or 52A of the Act must be A3 or A4 size, or in an electronic format, and include the following:

(a) a title;

(b) a linear scale;

(c) a north point;

(d) a legend;

(e) if the map contains map projections—details of the projections;

(f) if the maritime security plan to which the map relates details security regulated port boundaries—coordinates to clearly define those boundaries;

(g) if the maritime security plan to which the map relates details port security zone boundaries—coordinates to clearly define those boundaries;

(h) if inserts are used on the map—a numbered map for each insert corresponding to the number for the insert on the main map;

(i) the date the map was produced;

(j) the name of the person who created the map.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) Each map for a maritime security plan must be a separate map.

3.12 Protection of maritime security plans

A port operator and port facility operator must ensure that the maritime security plan for the operator is protected against unauthorised access, amendment and disclosure.

3.15 Port operator to give information

A port operator required to have a maritime security plan must give to each port facility operator conducting operations within the security regulated port:

(a) the information set out in regulation 3.35 (including contact details for the PSO); and

(b) the measures to be used by the port operator to inform persons of the location of maritime security zones established within the boundaries of the security regulated port; and

(c) the measures to confirm the identity of persons who are authorised to have access to maritime security zones established within the boundaries of the security regulated port.

3.20 Port facility operator to give information

(1) A port facility operator required to have a maritime security plan must give to the port operator of the security regulated port:

(a) the information set out in regulation 3.100 (including contact details for the PFSO); and

(b) the measures to be used by the port facility operator to inform persons of the location of any port security zones established within the boundaries of the port facility; and

(c) the measures to confirm the identity of persons who are authorised to have access to the port facility, to ships moored at the facility and to any port security zones established within the boundaries of the port facility.

(2) A port facility operator required to have a maritime security plan must also give to the port operator details of the boundaries of the facility.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 3.2—Port operators

3.30 General

A maritime security plan for a port operator must cover all matters of ship/port interface:

(a) that are to be conducted within the security regulated port; and

(b) that are not covered by a maritime security plan for any other maritime industry participant that conducts operations within, or in connection with, the security regulated port.

3.35 Port operator details

(1) A maritime security plan for a port operator must be accompanied by a document setting out the following information:

(a) name of the port operator;

(b) contact details for the port operator;

(c) name of the Chief Executive Officer of the port operator;

(d) name of the port for which the port operator has been designated;

(e) name of the port's harbour master;

(f) contact details for the harbour master;

(g) name or position of the person who is to be the PSO for the port;

(h) the contact details for the PSO.

(2) A port operator must, within 2 working days after the port operator becomes aware of a change in any of the information given under this regulation, notify the Secretary, in writing, of the change.

Penalty: 20 penalty units.

(3) An offence against subregulation (2) is an offence of strict liability.

3.40 Security assessments

In addition to the matters required under regulation 3.05, the security assessment that must be included in a maritime security plan for a port operator must include the following matters:

(a) a statement outlining the risk context or threat situation for the port;

(b) identification and evaluation of strategically important assets, infrastructure and operations that need to be protected;

(c) identification of possible risks or threats to assets, infrastructure and operations, and the likelihood and consequences of their occurrence;

(d) identification of existing security measures, procedures and operations;

(e) identification of gaps in port-wide security arrangements, including gaps arising from port infrastructure, human factors, policies and procedures;

Replaced Authorised Version registered 19/04/2024 F2021C00921

(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

3.45 Port security officer qualifications and responsibilities

A maritime security plan for a port operator must set out:

(a) the knowledge, skills and other requirements for the PSO; and

(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and

(c) the training that must be given to the PSO.

3.50 Other personnel with security role

(1) A maritime security plan for a port operator must identify, by reference to their positions, port personnel with, or who have been assigned, security duties and responsibilities in addition to those of the PSO.

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with:

(a) the knowledge, skills and other requirements for the security-related aspects of their positions; and

(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and

(c) the training that must be given to such personnel.

3.55 Matters that must be in plan

A maritime security plan for a port operator must address, in addition to the matters required under regulation 3.10, the following matters:

(a) measures to prevent unauthorised access to any port security zones established, or ship security zones declared, in the security regulated port;

(b) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations in the port;

(c) procedures for responding to any security directions given by the Secretary;

(d) procedures for evacuation of the port in case of security threats or breaches of security;

(e) procedures for drills and exercises associated with the plan;

(f) procedures for interfacing with ship security activities;

(g) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the port;

(h) procedures for reporting occurrences which threaten the security of the port;

(i) measures to ensure the security of the information contained in the plan;

Replaced Authorised Version registered 19/04/2024 F2021C00921

(j) procedures in case the ship security alert system of a ship is activated while in the security regulated port.

Note: A maritime security plan for a port operator must be accompanied by a map covering the whole security regulated port and showing the port security zones established within the port (see subsections 49(2) and (3) of the Act and regulation 3.90).

3.60 Consultation and communication

(1) A maritime security plan for a port operator must set out a mechanism for consultation:

(a) between the port operator and each of the maritime industry participants conducting operations within the security regulated port, for the purpose of coordinating their security-related activities; and

(b) between the port operator and its employees (or their representatives) regarding security measures and procedures to be implemented.

(2) A maritime security plan for a port operator must set out how the port operator will give notice under subsections 27(2) and 35(4) of the Act.

3.65 Maritime security level 1

A maritime security plan for a port operator must set out, in relation to maritime security level 1:

(a) the security measures, identified in the security assessment for the operation, for implementation at that level; and

(b) the measures that have been implemented; and

(c) a schedule for implementing the measures that have not been implemented; and

(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.

3.70 Maritime security levels 2 and 3

A maritime security plan for a port operator must set out, in relation to maritime security levels 2 and 3, the additional security measures that the operator will implement if the Secretary declares that maritime security level 2 or 3 is in force for the port.

3.75 Declarations of security

A maritime security plan for a port operator must provide for:

(a) the circumstances in which the operator will request a declaration of security with a ship; and

(b) the procedures for negotiating the security measures and responsibilities of the operator and of the ship in those circumstances; and

(c) how security measures identified in a declaration will be implemented to ensure compliance by the operator and the ship with their security plans and with the declaration.

Replaced Authorised Version registered 19/04/2024 F2021C00921

3.77 Land-side restricted zones

(1) If a port operator wishes the Secretary to establish a land-side restricted zone, the maritime security plan for the port operator must set out:

(a) the purpose for the proposed establishment of the zone; and

(b) the boundaries of the zone; and

(c) if applicable, the period when, or the circumstances in which, the zone is in force; and

(d) the security measures and procedures to be taken to control access into the zone by people, vehicles or things; and

(e) steps to be taken to inform people that a land-side restricted zone is in force and that entry into the zone without authority is an offence; and

(f) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (d) and (e).

(2) A maritime security plan for a port operator must set out security measures and procedures to monitor and control access to land-side restricted zones, including measures to detect and deter unauthorised access to those zones.

3.80 Water-side restricted zones

(1) If a port operator wishes the Secretary to establish a water-side restricted zone, the maritime security plan for the port operator must set out:

(a) the purpose for the proposed establishment of the zone; and

(b) the boundaries of the zone; and

(c) if applicable, the period when, or the circumstances in which, the zone is in force; and

(d) the security measures and procedures to be taken to control access into the zone by people, vessels or things; and

(e) steps to be taken to inform people that a water-side restricted zone is in force and that entry into the zone without authority is an offence; and

(f) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (d) and (e).

(2) A maritime security plan for a port operator must set out security measures and procedures to monitor and control access to water-side restricted zones, including measures to detect and deter unauthorised access to those zones.

3.85 Ship security zones

A maritime security plan for a port operator must set out security measures and procedures to monitor and control access to ship security zones, including measures to detect and deter unauthorised access to those zones.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 3.3—Port facility operators

3.100 Port facility operator details

A maritime security plan for a port facility operator must be accompanied by a document setting out the following information:

(a) name of the port facility operator;
(b) contact details for the port facility operator;
(c) name of the Chief Executive Officer of the port facility operator;
(d) name and location of the port facility;
(e) name of the port in which the facility is located;
(f) name or position of the person who is to be the PFSO for the facility;
(g) the contact details for the PFSO.

3.105 Details of PSO of security regulated ports

A maritime security plan for a port facility operator must be accompanied by a document setting out the name of, and contact details for, the PSO of the security regulated port in which the facility is located.

3.106 Obligation to keep information current

(1) A port facility operator must, within 2 working days after the port facility operator becomes aware of a change in any of the information given under regulation 3.100 or 3.105, notify the Secretary, in writing, of the change.

Penalty: 20 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

3.110 Security assessments

(1) In addition to the matters required under regulation 3.05, a security assessment for a port facility operator's operation must include the following matters:

(a) a statement outlining the risk context or threat situation for the port facility;
(b) identification and evaluation of important assets, infrastructure and operations that need to be protected;
(c) identification of possible risks or threats to assets, infrastructure and operations, and the likelihood and consequences of their occurrence;
(d) identification of existing security measures, procedures and operations;
(e) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;
(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) A security assessment for a port facility operator's operation must consider:
(a) the types of ships, and the types of cargoes transported by ships, served by the port facility; and
(b) any special risks or threats associated with such ships and cargoes.

3.115 PFSO qualifications and responsibilities

A maritime security plan for a port facility operator must set out:
(a) the knowledge, skills and other requirements for the PFSO; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to the PFSO.

3.120 Other personnel with security role

(1) A maritime security plan for a port facility operator must identify, by reference to their positions, port facility personnel with, or who have been assigned, security duties and responsibilities in addition to those of the PFSO.

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with:
(a) the knowledge, skills and other requirements for the security-related aspects of their positions; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to such personnel.

3.125 Matters that must be in plan

(1) A maritime security plan for a port facility operator must address, in addition to the matters required under regulation 3.10, the following matters:
(a) measures to prevent unauthorised carriage or possession of weapons or prohibited items in the facility or on board ships being loaded or unloaded at the facility;
(b) measures to prevent unauthorised access to the port facility, to ships moored at the facility and to any port security zones established within the boundaries of the port facility;
(c) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations in the port facility or ship/port interface;
(d) procedures for responding to any security directions given by the Secretary;
(e) procedures for evacuation of the port facility in case of security threats or breaches of security;
(f) procedures for drills and exercises associated with the plan;
(g) procedures for interfacing with ship security activities;

Replaced Authorised Version registered 19/04/2024 F2021C00921

(h) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the port facility;

(i) procedures for reporting occurrences which threaten the security of the port facility;

(j) measures to ensure the security of the information contained in the plan;

(k) measures to ensure security of cargo and of cargo handling equipment at the facility;

(l) procedures in case the ship security alert system of a ship is activated while in the security regulated port;

(m) procedures for facilitating:

(i) shore leave or relief of crew; and

(ii) access by visitors (including representatives of seafarers' welfare and of labour organisations).

(2) In determining appropriate measures for paragraphs (1)(a) and (b), the port facility operator must have regard to the special risks or threats associated with the types of ships, and the types of cargoes transported by ships, regularly served by the port facility.

Note: A maritime security plan for a port facility operator must be accompanied by a map showing any port security zones established within the facility (see paragraph 49(2)(a) of the Act and regulation 3.165).

3.130 Consultation

A maritime security plan for a port facility operator must set out, for the purpose of coordinating security-related activities, a mechanism for consultation:

(a) between the port facility operator and the port operator; and

(b) between the port facility operator and any stakeholder who may be affected by the implementation of the plan; and

(c) between the port facility operator and its employees (or their representatives) regarding security measures and procedures to be implemented.

3.135 Maritime security level 1

A maritime security plan for a port facility operator must set out, in relation to maritime security level 1:

(a) the security measures, identified in the security assessment for the operation, for implementation at that level; and

(b) the measures that have been implemented; and

(c) a schedule for implementing the measures that have not been implemented; and

(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.

Replaced Authorised Version registered 19/04/2024 F2021C00921

3.140 Maritime security levels 2 and 3

A maritime security plan for a port facility operator must set out, in relation to maritime security levels 2 and 3, the additional security measures that the operator will implement if the Secretary declares that maritime security level 2 or 3 is in force for the port.

3.145 Declarations of security

A maritime security plan for a port facility operator must provide for:

(a) the circumstances in which the operator will request a declaration of security with a ship; and

(b) the procedures for negotiating the security measures and responsibilities of the operator and of the ship in those circumstances; and

(c) how security measures identified in a declaration will be implemented to ensure compliance by the operator and the ship with their security plans and with the declaration.

3.150 Land-side restricted zones

(1) If a port facility operator wishes the Secretary to establish a land-side restricted zone, the maritime security plan for the port facility operator must set out:

(a) the purpose for the proposed establishment of the zone; and

(b) the boundaries of the zone; and

(c) if applicable, the period when, or the circumstances in which, the zone is in force; and

(d) the security measures and procedures to be taken to control access into the zone by people, vehicles or things, (including measures relating to the entry, parking, loading and unloading of vehicles, and the movement and storage of cargo, stores and baggage); and

(e) steps to be taken to inform people that a land-side restricted zone is in force and that entry into the zone without authority is an offence; and

(f) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (d) and (e).

(2) A maritime security plan for a port facility operator must set out security measures and procedures to monitor and control access to land-side restricted zones, including measures to detect and deter unauthorised access to those zones.

3.155 Cleared zones

(1) If a port facility operator wishes the Secretary to establish a cleared zone, the maritime security plan for the port facility operator must set out:

(a) the purpose for the proposed establishment of the zone; and

(b) the boundaries of the zone; and

(c) if applicable, the period when, or the circumstances in which, the zone is in force; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(d) the security measures and procedures to be taken to control access into the zone by people, vehicles or things, (including measures relating to the entry, parking, loading and unloading of vehicles, and the movement and storage of cargo, stores and baggage); and

(e) steps to be taken to inform people that a cleared zone is in force and that is an offence to enter the zone without the required screening and clearance; and

(f) the name or position of each person responsible for the security measures, procedures or steps referred to in paragraphs (d) and (e).

(2) A maritime security plan for a port facility operator must set out measures and procedures to ensure that persons and goods are screened and cleared in accordance with these Regulations before they are allowed to enter and remain in any cleared zone established in the port facility.

3.160 Passenger ships

(1) If a port facility operator wishes to operate a port facility for use in connection with the loading or unloading of security regulated ships that are passenger ships, the maritime security plan for the port facility operator must set out:

(a) procedures for screening and clearing persons and their baggage; and

(b) procedures for detecting weapons and prohibited items; and

(c) procedures for surrender and dealing with weapons and prohibited items that are detected; and

(d) the name or position of the person or persons responsible for the procedures referred to in paragraphs (a), (b) and (c).

(1A) Paragraph (1)(a) applies in relation to the loading or unloading of the following:

(a) a regulated Australian ship of a kind mentioned in paragraph 16(1)(a) of the Act;

(b) a regulated foreign ship of a kind mentioned in subparagraph 17(1)(b)(i) of the Act.

(2) If in a port facility there is no screening point through which persons who are required to be screened and cleared to board a security regulated ship must pass, the procedures for screening and clearing persons referred to in paragraph (1)(a) must include procedures for making arrangements, between the port facility operator and the master of a ship that is moored at the facility, for persons to be screened and cleared on board the ship immediately after they board.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 4—Ship security plans and ISSCs

Division 4.1—Preliminary

Note: This Division heading is reserved for future use.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 4.2—Matters to be dealt with in ship security plan

4.20 Identification of ship

A ship security plan must be accompanied by a document setting out the following information about the ship:

(a) name of the ship;
(b) the ship's official number;
(c) if the plan is for a regulated Australian ship that is used for overseas voyages—the ship's IMO ship identification number;
(d) any other distinctive numbers or letters that identify the ship;
(e) type of ship;
(f) radio call sign;
(g) date and port of registry;
(h) year built;
(i) deadweight tonnage;
(j) gross tonnage;
(k) length and breadth of ship;
(l) summer draft;
(m) number of crew;
(n) number of passenger berths;
(o) whether the ship is engaged in overseas or inter-State voyages.

Note: For the definition of ***official number***, see subregulation 1.03(1).

4.25 Security assessments

A ship security assessment for a regulated Australian ship must include the following matters:

(a) the date when the assessment was completed or reviewed;
(b) the scope of the assessment, including assets, infrastructure and operations assessed;
(c) a summary of how the assessment was conducted, including details of the risk management process adopted;
(d) the skills and experience of the key persons who completed or participated in the assessment;
(e) the results of the examination and evaluation of the existing shipboard protective measures, procedures and operations;
(f) a statement outlining the risk context or threat situation for the ship, including consideration of trading routes;
(g) identification and evaluation of key shipboard operations that need to be protected;
(h) identification of possible risks or threats to the key shipboard operations and the likelihood and consequences of their occurrence;
(i) identification of existing security measures, procedures and operations;

Replaced Authorised Version registered 19/04/2024 F2021C00921

(j) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;

(k) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

4.30 Ship operator, CSO and SSO

(1) A ship security plan must be accompanied by a document setting out the following information:

(a) the name of the ship operator;

(b) the name of the Chief Executive Officer of the ship operator;

(c) the name or position of the person who is to be the CSO for the ship;

(d) the contact details for the CSO;

(e) the name and contact details for the SSO.

(2) A ship security plan may set out duties and responsibilities of a CSO or SSO that are in addition to the duties and responsibilities of a CSO and SSO in sections 11.2 and 12.2, respectively, of Part A of the ISPS Code.

(3) A ship security plan must set out how the CSO will communicate with the master of the ship if the Secretary or a maritime industry participant acting on behalf of the Secretary:

(a) gives notice that a maritime security level is in force for the ship; or

(b) gives a security direction to the ship.

4.31 Obligation to keep information current

(1) A ship operator must, within 2 working days after the ship operator becomes aware of a change in any of the information given under regulation 4.20 or 4.30, notify the Secretary, in writing, of the change.

Penalty: 20 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

4.35 Shore-based personnel and crew with security role

(1) A ship security plan must identify, by reference to their positions, shore-based personnel and crew with, or who have been assigned, security duties and responsibilities.

(2) The security duties and responsibilities of personnel and crew so identified must be set out in the plan, together with:

(a) the knowledge, skills and other requirements for the security-related aspects of their positions; and

(b) the training or qualifications that satisfy the requirements referred to in paragraph (a).

Replaced Authorised Version registered 19/04/2024 F2021C00921

4.40 Training

A ship security plan must set out the training that a CSO, SSO, and shore-based personnel and crew referred to in regulation 4.35 must receive.

4.45 Matters that must be in plan

A ship security plan must address the following matters:

(a) measures to prevent unauthorised carriage or possession of weapons or prohibited items on board the ship;

(b) identification of on-board security zones;

(c) measures to prevent unauthorised access to the ship and any on-board security zones;

(d) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations of ship/port interface;

(e) procedures for:

(i) acknowledging, and responding to, directions given by the Secretary or a contracting government; and

(ii) acknowledging notifications of the security level in force from the Secretary or a contracting government;

(f) procedures for evacuation of the ship in case of security threats or breaches of security;

(g) procedures for drills and exercises associated with the plan;

(h) procedures for interfacing with port, port facility and offshore facility security activities;

(i) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the ship;

(j) procedures for reporting occurrences which threaten the security of the ship;

(k) measures to ensure the security of the information contained in the plan.

4.50 Maritime security level 1

A ship security plan must set out, in relation to maritime security level 1:

(a) the security measures identified in the ship security assessment for implementation at that level; and

(b) the measures that have been implemented; and

(c) a schedule for implementing the measures that have not been implemented; and

(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.

4.55 Maritime security levels 2 and 3

A ship security plan must set out, in relation to maritime security levels 2 and 3:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(a) the security measures identified in the ship security assessment for implementation at those levels; and
(b) the additional security measures that the ship will implement if the Secretary declares that maritime security level 2 or 3 is in force for the ship.

4.60 Declarations of security

A ship security plan must provide for:
(a) the circumstances in which the ship will request a declaration of security with another ship or person; and
(b) the procedures for negotiating the security measures and responsibilities of the ship and of the other ship or person in those circumstances; and
(c) how security measures identified in a declaration will be implemented to ensure compliance by the parties with their security plans and with the declaration.

4.65 On-board security zones

(1) If the ship operator for a regulated Australian ship wishes the Secretary to establish an on-board security zone for the ship, the ship security plan must set out:
(a) the purpose for the proposed establishment of the zone; and
(b) the boundaries of the zone; and
(c) the security measures and procedures to be taken to control access into the zone by people or things; and
(d) steps to be taken to inform people that the on-board security zone has been established and that entry into the zone without authority is an offence; and
(e) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (c) and (d); and
(f) if applicable, the period when, or the circumstances in which, the zone is in force.

(2) A ship security plan must set out security measures and procedures to monitor and control access to on-board security zones, including measures to detect and deter unauthorised access to those zones.

4.70 Security of ship in non-ISPS Code compliant ports

(1) This regulation applies if it is envisaged by the ship operator that a regulated Australian ship may call at ports or locations that are not port facilities or are port facilities the operators of which are not required to have, or do not have, security plans.

(2) A ship security plan must outline specific measures that will be implemented if the ship calls at ports or locations described in subregulation (1) so that any risks associated with those ports or locations are not transferred to the ship.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Regulation 4.75

4.75 Security of ship in exceptional circumstances

A ship security plan must give sufficient guidance on how the security of the ship will be maintained in exceptional circumstances such as search and rescue operations, humanitarian crises, extreme weather conditions and other emergencies.

4.80 Pre-entry information

(1) A ship security plan for a regulated Australian ship that is used for overseas voyages must set out the procedures for giving pre-entry information in accordance with subregulations (2) and (3).

(2) The master of a regulated Australian ship that is due to arrive, from a place outside Australia, at a port in Australia must give the following information (***pre-entry information***) to a customs officer:

(a) confirmation that a valid ISSC is on board the ship;
(b) the name of the authority that issued the ship's ISSC;
(c) the date when the ISSC expires;
(d) the maritime security level at which the ship is operating;
(e) the last 10 ports of call where the ship conducted ship/port interface;
(f) whether the ship operated at a security level different from that in paragraph (d), engaged in ship to ship activity, or implemented any special or additional security measures, in the last 10 ports of call;
(g) if known, the next 4 ports of call of the ship (whether in or outside Australia) after the port in relation to which the information is being given.

(3) Pre-entry information must be given at the time the crew report required under section 64ACB of the *Customs Act 1901* is given in relation to the port.

Note: Section 6 of the *Navigation Act 1912* defines overseas voyage as follows:

overseas voyage, in relation to a ship, means a voyage in the course of which the ship travels between:

(a) a port in Australia and a port outside Australia;
(b) a port in Australia and a place in the waters of the sea above the continental shelf of a country other than Australia;
(c) a port outside Australia and a place in the waters of the sea above the continental shelf of Australia;
(d) a place in the waters of the sea above the continental shelf of Australia and a place in the waters of the sea above the continental shelf of a country other than Australia;
(e) ports outside Australia; or
(f) places beyond the continental shelf of Australia.

4.85 Maritime transport or offshore facility security incidents

A ship security plan must set out procedures for:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(a) reporting maritime transport or offshore facility security incidents to the Secretary; and
(b) responding to security threats and breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface or the ship/facility interface.

4.90 Security equipment

A ship security plan must:
(a) include a list of the security equipment on board the ship; and
(b) describe the measures to ensure the inspection, testing, calibration and maintenance of security equipment; and
(c) set out the frequency for testing and calibration of security equipment; and
(d) set out procedures to ensure that only correctly calibrated security equipment is used on board the ship.

4.95 On-board systems

(1) A ship security plan must include information about the following systems on board the ship:
(a) external and internal communications systems;
(b) surveillance, identification, monitoring and reporting systems;
(c) tracking and positional systems.

(2) If a ship is provided with a ship security alert system, the ship security plan must:
(a) describe the operational characteristics of the system; and
(b) describe the ship security alert that will be transmitted from the system; and
(c) describe the performance standards to which the system must conform, being standards not below those adopted by the IMO; and
(d) set out the procedures, instructions and guidance for using, testing, activating, de-activating and resetting the system, and for preventing false alarms.

4.100 Ship security records

A ship security plan must set out:
(a) the ship security records that are required to be kept on, by and for the ship in accordance with regulation 1.55; and
(b) a plan for keeping and preserving ship security records; and
(c) the procedures for making those records available for inspection in accordance with subregulation 1.55(3A).

4.105 Security plan audits and reviews

A ship security plan must set out:
(a) a schedule of security plan audits; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(b) the circumstances, in addition to the occurrence of a maritime transport security incident, following which a security plan review must be conducted; and

(c) the procedures for conducting a security plan audit, including a process for selecting auditors who are independent of the matters being audited; and

(d) the procedures for conducting a security plan review, including a process for consultation during the review.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 4.3—Form of ship security plan

4.110 Statement about authority of master

A ship security plan must include a statement to the following effect:

‘The master of the ship has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance of the ship operator or of any contracting government to the SOLAS Convention, as may be necessary.’.

Note: For the definition of ***SOLAS Convention***, see section 10 of the Act.

4.115 Protection of plan

The ship operator for a regulated Australian ship must ensure that the ship security plan for the ship is protected against unauthorised access, amendment and disclosure.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 4.4—Ship security plans—exemptions, approvals, revisions and cancellations

4.120 Application for exemption—prescribed requirements

(1) For subsection 61A(2) of the Act, this regulation prescribes requirements for an application for an exemption from the operation of Division 2 of Part 4 of the Act.

Form of application

(2) The application must be made in writing to the Secretary.

Content of application

(3) If an ISSC is in force for the ship, the application must include a copy of the ISSC.

(4) The application must include the following information:
- (a) the ship's:
  - (i) name; and
  - (ii) type; and
  - (iii) operating company; and
  - (iv) gross tonnage; and
  - (v) official number; and
- (b) if an IMO ship identification number has been assigned to the ship—that number;
- (c) any other number that uniquely identifies the ship, composed of:
  - (i) letters; or
  - (ii) numbers; or
  - (iii) a combination of letters and numbers;
- (d) the name of the ship's:
  - (i) master; and
  - (ii) SSO; and
  - (iii) CSO; and
  - (iv) port of registry;
- (e) whether a ship security plan is in force for the ship;
- (f) information about the requested exemption, including:
  - (i) the commencement date and expiry date of the period in which the exemption will, if granted, have effect; and
  - (ii) the ship's last 10 ports of call; and
  - (iii) the ship's last port of call before the exemption will, if granted, commence; and
  - (iv) the ship's first port of call after the exemption will, if granted, commence; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(v) the reasons an exemption is required; and

(vi) details of all voyages that the ship operator intends the ship to undertake without a ship security plan, including details of the intended route and any intended ports of call along the route; and

(vii) whether the ship will carry passengers during all or part of the period in which the exemption will, if granted, have effect; and

(viii) whether the ship will carry cargo during all or part of the period in which the exemption will, if granted, have effect;

(ix) any other information that the ship operator would like the Secretary to consider in deciding whether or not to grant the exemption.

Note: Information about the IMO's ship identification number scheme is available at http://www.imo.org.

4.125 Matters the Secretary must consider

For subsection 61A(3) of the Act, the following matters are prescribed:

(a) the information mentioned in paragraphs 4.120(4)(a) to (f);

(b) whether the voyage for which the ship operator has applied for an exemption is a rare occurrence;

(c) whether the circumstances that give rise to the need for the exemption are exceptional;

(d) whether there is a threat of a terrorist act against the ship;

(e) whether there is a risk of the ship being used to facilitate a terrorist act or an unlawful interference with maritime transport or offshore facilities;

(f) whether granting an exemption will bring an increased risk of a terrorist act against:

(i) any Australian port; or

(ii) any other vessel;

(g) whether the ship will carry passengers during all or part of the period in which the exemption will, if granted, have effect;

(h) whether the ship will carry cargo during all or part of the period in which the exemption will, if granted, have effect;

(i) whether the ship operator has applied for an exemption to undertake a voyage for the purpose of:

(i) delivery of a ship; or

(ii) maintenance, refitting or any other modification of a ship.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 4.5—International ship security certificates

4.140 Applications for ISSC

(1) For subsection 81(2) of the Act, an application for an ISSC must be in writing and must:

(a) identify the ship by means of the following:

(i) the name of the ship;

(ii) the ship's official number;

(iii) if the ship is used for overseas voyages—the ship's IMO ship identification number;

(iv) any other distinctive numbers or letters that identify the ship; and

(b) include a statement that a ship security plan is in force for the ship.

(2) The application must also state when the ship may be inspected for the purpose of determining whether the ship meets the requirements necessary for ISSC verification.

Note: For the definition of ***official number***, see subregulation 1.03(1).

4.145 Inspections by authorised persons

The ISSC for a regulated Australian ship must be made available for inspection at the request of a person who is authorised by a contracting government to request information about, or in connection with, whether a valid ISSC is in force for the ship.

Note: For the power of maritime security inspectors and duly authorised officers to inspect ISSCs, see subparagraphs 139(2)(e)(i) and 148(2)(c)(i) of the Act, respectively.

4.150 Application for exemption—prescribed requirements

(1) For subsection 79A(2) of the Act, this regulation prescribes requirements for an application for an exemption from the operation of Division 6 of Part 4 of the Act.

Form of application

(2) The application must be made in writing to the Secretary.

Content of application

(3) If an ISSC is in force for the ship, the application must include a copy of the ISSC.

(4) The application must include the following information:

(a) the ship's:

(i) name; and

(ii) type; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(iii) operating company; and
(iv) gross tonnage; and
(v) official number; and

(b) if an IMO ship identification number has been assigned to the ship—that number;

(c) any other number that uniquely identifies the ship, composed of:
(i) letters; or
(ii) numbers; or
(iii) a combination of letters and numbers;

(d) the name of the ship's:
(i) master; and
(ii) SSO; and
(iii) CSO; and
(iv) port of registry;

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

(f) information about the requested exemption, including:
(i) the commencement date and expiry date of the period in which the exemption will, if granted, have effect; and
(ii) the ship's last 10 ports of call; and
(iii) the ship's last port of call before the exemption will, if granted, commence; and
(iv) the ship's first port of call after the exemption will, if granted, commence; and
(v) the reasons an exemption is required; and
(vi) details of all voyages that the ship operator intends to undertake without an ISSC, including details of the intended route and any intended ports of call along the route; and
(vii) whether the ship will carry passengers during all or part of the period in which the exemption will, if granted, have effect; and
(viii) whether the ship will carry cargo during all or part of the period in which the exemption will, if granted, have effect; and
(ix) any other information that the ship operator would like the Secretary to consider in deciding whether or not to grant the exemption.

Note: Information about the IMO's ship identification number scheme is available at http://www.imo.org.

4.155 Matters the Secretary must consider

For subsection 79A(3) of the Act, the following matters are prescribed:

(a) the information mentioned in paragraphs 4.150(4)(a) to (f);

(b) whether the voyage for which the ship operator has applied for an exemption is a rare occurrence;

(c) whether the circumstances that give rise to the need for the exemption are exceptional;

(d) whether there is a threat of a terrorist act against the ship;

Replaced Authorised Version registered 19/04/2024 F2021C00921

(e) whether there is a risk of the ship being used to facilitate a terrorist act or an unlawful interference with maritime transport or offshore facilities;

(f) whether granting an exemption will bring an increased risk of a terrorist act to:

(i) any Australian port; or

(ii) any other vessel;

(g) whether the ship will carry passengers during all or part of the period in which the exemption will, if granted, have effect;

(h) whether the ship will carry cargo during all or part of the period in which the exemption will, if granted, have effect;

(i) whether the ship operator has applied for an exemption to undertake a voyage for the purpose of:

(i) delivery of a ship; or

(ii) maintenance, refitting or any other modification of a ship.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 5—Regulated foreign ships

Division 5.1—Obligations

5.10 Pre-arrival information

(1) For subsection 92(2) of the Act, pre-arrival information must be given to a customs officer by the master of a ship that is due to arrive, from a place outside Australia, at a port in Australia (whether the first port or any subsequent port on the same voyage) at the time the crew report required under section 64ACB of the *Customs Act 1901* is given in relation to the port.

(2) For the definition of ***pre-arrival information*** in subsection 92(3) of the Act, the following are prescribed:

(a) confirmation that a valid ISSC, or approved ISSC equivalent under subsection 91(3) of the Act, is on board the ship;

(b) the name of the authority that issued the ship's ISSC or approved ISSC equivalent;

(c) the date when the ISSC or approved ISSC equivalent expires;

(d) the security level at which the ship is operating;

(e) the last 10 ports of call where the ship conducted ship/port interface;

(f) whether the ship operated at a security level different from that in paragraph (d), engaged in ship to ship activity, or implemented any special or additional security measures, in the last 10 ports of call;

(g) if known, the next 4 ports of call of the ship (whether in or outside Australia) after the port in relation to which the information is being given.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 5.2—Control directions

5.20 Requirement for consultation

If it is reasonable and practicable to do so, the Secretary must consult with the following about giving a control direction that relates to the movement of ships within, or in or out of, a security regulated port:

(a) maritime industry participants who will be affected by the direction;

(b) agencies of the Commonwealth, a State or Territory whose operations in the port will be affected by the direction;

(c) persons, other than those mentioned in paragraph (a) or (b), who need to implement, or comply with, the direction.

Examples: For paragraph (c), harbour masters and PSOs.

5.25 Giving control directions (Act s 99(7))

The Secretary must give a control direction to the ship operator for, or the master of, a regulated foreign ship:

(a) orally (for example, by telephone or radio communication); or

(b) in writing; or

(c) by electronic transmission (for example, by fax or e-mail).

Note: Under subsection 99(5) of the Act, a control direction has no effect until the Secretary commits the direction to writing.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 5A—Offshore security plans

Division 5A.1—Preliminary

5A.05 Common requirements for security assessments

A security assessment for an offshore security plan must include the following matters:

(a) the date when the assessment was completed or reviewed;

(b) the scope of the assessment, including assets, infrastructure and operations assessed;

(c) a summary of how the assessment was conducted, including details of the risk management process adopted;

(d) the skills and experience of the key persons who completed or participated in the assessment.

5A.10 Common requirements for security plan audits and reviews

An offshore security plan for an offshore industry participant must set out:

(a) a schedule of security plan audits; and

(b) the circumstances, in addition to the occurrence of a maritime transport or offshore facility security incident, following which a security plan review must be conducted; and

(c) the procedures for conducting a security plan audit, including a process for selecting auditors who are independent of the matters being audited; and

(d) the procedures for conducting a security plan review, including a process for consultation during the review.

5A.15 Offshore facility operator to give information

The operator of an offshore facility must give to each offshore service provider conducting operations at the facility:

(a) the information set out in regulation 5A.30; and

(b) the measures to be used by the operator to inform persons of the location of offshore security zones established by the operator for the facility; and

(c) the measures to confirm the identity of persons who are authorised to have access to the zones.

Note: The information for paragraph (a) must include the contact details for the OFSO.

5A.20 Offshore service provider to give information

An offshore service provider that is required to have a security plan must give to the operator of each offshore facility to which the service provider conducts operations:

(a) the information set out in regulation 5A.120; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(b) a description of the boundaries of the service provider's supply base and the arrangements made to ensure the security of goods that are to be transported to the facility; and

(c) details of each vessel or aircraft operated by the service provider to service the facility; and

(d) the measures to be used by the service provider to inform persons of the security arrangements, including any security zones, at the service provider's supply base; and

(e) details of the measures to be used to confirm the identity of persons who are allowed to enter:

(i) the supply base; and

(ii) any security zone established in the supply base; and

(iii) a vessel or aircraft operated by the service provider.

Note: The information for paragraph (a) must include the contact details for the OSPSO.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 5A.2—Offshore facility operators

Subdivision 5A.2.1—Matters to be dealt with in plan

5A.25 Offshore security plans (Act s 100H)

For section 100H of the Act, this Subdivision prescribes the matters that are to be dealt with in an offshore security plan for an offshore facility operator.

Note: An offshore facility operator that has more than 1 facility may prepare 1 plan for each facility, or 1 plan covering a number of facilities that are in the same area, and are physically and operationally similar, and that have identical risk assessments.

5A.30 Offshore facility operator details

An offshore security plan for an offshore facility operator must be accompanied by a document setting out the following information:

(a) the name of the operator;
(b) contact details for the operator;
(c) name of the Chief Executive Officer and the HSO of the operator;
(d) the name and location of each facility;
(e) name or position of the person who is to be the OFSO for each facility covered by the plan;
(f) the contact details for the OFSO of the operator.

5A.35 Details of offshore service providers

An offshore security plan for an offshore facility operator must be accompanied by a document setting out the name of, and contact details for, the OSPSO of each offshore service provider conducting operations at each facility.

5A.40 Obligation to keep information current

(1) An offshore facility operator must, within 2 working days after becoming aware of a change in any of the information given under regulation 5A.30 or 5A.35, notify the Secretary, in writing, of the change.

Penalty: 20 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

5A.45 Security assessments

(1) In addition to the matters required under regulation 5A.05, a security assessment for an offshore facility operator's operation must include the following matters:

(a) a statement outlining the risk context or threat situation for each facility;
(b) identification and evaluation of important assets, infrastructure and operations that need to be protected;

Replaced Authorised Version registered 19/04/2024 F2021C00921

(c) identification of possible risks or threats to assets, infrastructure and operations, and the likelihood and consequences of their occurrence;
(d) identification of existing security measures, procedures and operations;
(e) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;
(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

(2) A security assessment for an offshore facility operator's operation must consider:
(a) the types of vessels or aircraft used, and the types of cargoes transported, in operations to and from each offshore facility; and
(b) any special risks or threats associated with the vessels, aircraft and cargoes.

5A.50 OFSO qualifications and responsibilities

An offshore security plan for an offshore facility operator must set out:
(a) the knowledge, skills and other requirements for the OFSO; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to the OFSO.

5A.55 Other personnel with security role

(1) An offshore security plan for an offshore facility operator must identify, by reference to their positions, personnel who have been assigned security duties and responsibilities in addition to those of the OFSO.

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with:
(a) the knowledge, skills and other requirements for the security-related aspects of their positions; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to such personnel.

5A.60 Matters that must be in plan

(1) An offshore security plan for an offshore facility operator must address, in addition to the matters required under regulation 5A.05, the following matters:
(a) measures to prevent unauthorised carriage or possession of weapons or prohibited items on a facility or on board vessels or aircraft interfacing with a facility;
(b) measures to prevent unauthorised access to:
(i) an offshore security zone established within and around a security regulated offshore facility; or

Replaced Authorised Version registered 19/04/2024 F2021C00921

(ii) a ship security zone declared to operate around a security regulated ship while the ship is in the vicinity of a security regulated offshore facility and is engaged in any activity in relation to the facility;

(c) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations at a facility;

(d) procedures for responding to security threats or breaches of security occurring during any interface between a vessel or aircraft and a facility;

(e) procedures for responding to any security directions given by the Secretary;

(f) procedures for evacuation of each facility in case of security threats or breaches of security;

(g) procedures for drills and exercises associated with the plan;

(h) procedures for interfacing with the security activities of other maritime industry participants and operators of any aircraft that may land on or near a facility;

(i) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to a facility;

(j) procedures for reporting occurrences which threaten the security of a facility;

(k) measures to ensure the security of the information contained in the plan;

(l) measures to ensure the security of cargo and of cargo handling equipment at a facility;

(m) procedures in case the ship security alert system of a ship is activated while it is near a facility;

(n) procedures to be followed when an offshore facility is directly connected to, or engaging in any activity with, a vessel such as a floating hotel, mobile drilling unit or construction barge.

(2) In determining appropriate measures for paragraphs (1)(a) and (b), the facility operator must have regard to the special risks or threats associated with the types of vessels and aircraft used to provide services for each offshore facility and the types of cargo carried by the vessels and aircraft.

5A.65 Consultation

An offshore security plan for an offshore facility operator must set out, for the purpose of coordinating security-related activities, a mechanism for consultation between the offshore facility operator and:

(a) each offshore industry participant conducting operations at (or interfacing with) a facility and any other stakeholder who may be affected by the implementation of the plan; and

(b) the operator's employees (or their representatives) regarding security measures and procedures to be implemented.

Replaced Authorised Version registered 19/04/2024 F2021C00921

5A.70 Maritime security level 1

An offshore security plan for an offshore facility operator must set out, in relation to maritime security level 1:

(a) the security measures, identified in the security assessment for the operation, for implementation at that level; and

(b) the measures that have been implemented; and

(c) a schedule for implementing the measures that have not been implemented; and

(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.

5A.75 Maritime security levels 2 and 3

An offshore security plan for an offshore facility operator must set out, in relation to maritime security levels 2 and 3, the additional security measures that the operator will implement if the Secretary declares that maritime security level 2 or 3 is in force for a facility of the operator.

5A.80 Declarations of security

An offshore security plan for an offshore facility operator must provide for:

(a) the circumstances in which the operator will request a declaration of security with another offshore industry participant; and

(b) the procedures for negotiating the security measures and responsibilities of the operator and the participant in those circumstances; and

(c) how security measures identified in a declaration will be implemented to ensure compliance by the operator and the participant with their security plans and with the declaration.

5A.85 Offshore facility zone

(1) If an offshore facility operator wishes the Secretary to establish an offshore facility zone for a facility, the offshore security plan for the operator must set out:

(a) the boundaries of the zone; and

(b) the security measures and procedures to be taken to control access into the zone by people, aircraft or things; and

(c) steps to be taken to inform people that an offshore facility zone is in force and that entry into the zone without authority is an offence; and

(d) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (b) and (c).

(2) The security plan must set out security measures and procedures to monitor and control access to the zone, including measures to detect and deter unauthorised access to the zone.

Replaced Authorised Version registered 19/04/2024 F2021C00921

5A.90 Offshore water-side zone

(1) If an offshore facility operator wishes the Secretary to establish an offshore water-side zone for a facility, the offshore security plan for the operator must set out:

(a) the boundaries of the zone; and

(b) the security measures and procedures to be taken to control access into the zone by people, vessels, aircraft or things; and

(c) steps to be taken to inform people that an offshore water-side zone is in force and that entry into the zone without authority is an offence; and

(d) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (b) and (c).

(2) The security plan must set out security measures and procedures to monitor and control access to the zone, including measures to detect and deter unauthorised access to the zone.

5A.92 Ship security zones

An offshore security plan for an offshore facility operator must set out security measures and procedures to monitor and control access to ship security zones, including measures to detect and deter unauthorised access to those zones.

Subdivision 5A.2.2—Form of plan

5A.95 Requirements for plans (Act s 100I)

For section 100I of the Act, this Subdivision sets out requirements for the preparation of an offshore security plan.

5A.100 Information for offshore security plans

The information that must accompany an offshore security plan for an offshore facility operator must:

(a) show the location (including the geographical coordinates) of each facility in a way that enables the Secretary to gazette the location of the facility; and

(b) include a diagram of a size and scale of each facility and surrounding water that shows the layout of the facility and of any offshore security zone.

5A.105 Protection of plan

An offshore facility operator must ensure that the offshore security plan for the operator's facility is protected against unauthorised access, amendment and disclosure.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 5A.3—Offshore service providers

Subdivision 5A.3.1—Preliminary

5A.110 Service providers to have offshore security plans (Act s 100B)

(1) For paragraph 100B (b) of the Act, an offshore industry participant that is an offshore service provider is prescribed.

(2) However subregulation (1) does not apply to a service provider if:
  (a) the activities of the service provider are covered by the offshore security plan for an offshore facility operator (the ***covering plan***) and the service provider has agreed in writing to the activities being covered by the covering plan; or
  (b) both of the following apply:
    (i) the activities of the service provider are covered by a maritime security plan, or a transport security program within the meaning given in the *Aviation Transport Security Act 2004*;
    (ii) the service provider has reviewed the plan and, if necessary, amended it to ensure that the provider satisfies the relevant requirements for offshore service providers under these Regulations.

Note: Section 100E of the Act deals with the activities of offshore industry participants being covered by offshore security plans of other offshore industry participants.

Subdivision 5A.3.2—Matters to be dealt with in plan

5A.115 Offshore security plans (Act s 100H)

For section 100H of the Act, this Subdivision prescribes the matters that are to be dealt with in an offshore security plan for an offshore service provider.

5A.120 Offshore service provider details

An offshore security plan for an offshore service provider must be accompanied by a document setting out the following information:
  (a) the name of the service provider;
  (b) contact details for the service provider;
  (c) name of the Chief Executive Officer of the service provider;
  (d) name of each port or airport:
    (i) where the service provider has a supply base; or
    (ii) from which the service provider operates;
  (e) name or position of the person who is to be the OSPSO for the service provider;
  (f) the contact details of the OSPSO of the service provider.

Replaced Authorised Version registered 19/04/2024 F2021C00921

5A.125 Details of other offshore industry participants

An offshore security plan for an offshore service provider must be accompanied by a document setting out the name of, and contact details for:

(a) each PSO of a security regulated port and airport security contact officer (within the meaning given in the *Aviation Transport Security Act 2004*) of a security controlled airport (within the meaning given in that Act):
  (i) where the service provider has a supply base; or
  (ii) from which the service provider operates; and
(b) each OFSO of a security regulated offshore facility serviced by the service provider.

5A.130 Obligation to keep information current

(1) An offshore service provider must, within 2 working days after becoming aware of a change in any of the information given under regulation 5A.120 or 5A.125, notify the Secretary, in writing, of the change.

Penalty: 20 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

5A.135 Security assessments

In addition to the matters required under regulation 5A.05, a security assessment for an offshore service provider must include the following matters:

(a) a statement outlining the risk context or threat situation for the offshore service provider;
(b) identification and evaluation of important assets, infrastructure and operations that need to be protected;
(c) identification of possible risks or threats to assets, infrastructure and operations, and the likelihood and consequences of their occurrence;
(d) identification of existing security measures, procedures and operations;
(e) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;
(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

5A.140 OSPSO qualifications and responsibilities

An offshore security plan for an offshore service provider must set out:

(a) the knowledge, skills and other requirements for the OSPSO; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to the OSPSO.

Replaced Authorised Version registered 19/04/2024 F2021C00921

5A.145 Other personnel with security role

(1) An offshore security plan for an offshore service provider must identify, by reference to their positions, personnel who have been assigned security duties and responsibilities in addition to those of the OSPSO.

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with:
  (a) the knowledge, skills and other requirements for the security-related aspects of their positions; and
  (b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
  (c) the training that must be given to such personnel.

5A.150 Matters that must be in plan

(1) An offshore security plan for an offshore service provider must address, in addition to the matters required under regulation 5A.05, the following matters:
  (a) measures to prevent unauthorised carriage or possession of weapons or prohibited items at a supply base of the service provider or on board vessels or aircraft operated by the service provider;
  (b) measures to prevent unauthorised access to a supply base of, or a vessel or aircraft operated by, the service provider;
  (c) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations of the offshore service provider;
  (d) procedures for responding to security threats or breaches of security occurring during any interface between a vessel or aircraft and a facility;
  (e) procedures for responding to any security directions given by the Secretary;
  (f) procedures for evacuation of a supply base of the service provider in case of security threats or breaches of security;
  (g) procedures for drills and exercises associated with the plan;
  (h) procedures for interfacing with the security activities of vessels and offshore facilities serviced by the service provider;
  (i) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to a relevant facility and to the service provider;
  (j) procedures for reporting occurrences which threaten the security of the offshore facility or the offshore service provider;
  (k) measures to ensure the security of the information contained in the plan;
  (l) measures to ensure security of passengers, cargo and cargo handling equipment under the control of the offshore service provider;
  (m) procedures in case the ship security alert system of a ship is activated while interfacing with the service provider.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) In determining appropriate measures for paragraph (1)(a) and (b), the service provider must have regard to the special risks or threats associated with the types of vessels and aircraft and the types of cargoes transported by vessels and aircraft serving an offshore facility.

5A.155 Consultation

An offshore security plan for an offshore service provider must set out, for the purpose of coordinating security-related activities, a mechanism for consultation between the service provider and:

(a) each offshore facility operator serviced by the service provider; and

(b) the operator of each security regulated port and each airport from which the service provider operates; and

(c) any other stakeholder who may be affected by the implementation of the plan; and

(d) the service provider's employees (or their representatives), regarding security measures and procedures to be implemented.

5A.160 Maritime security level 1

An offshore security plan for an offshore service provider must set out, in relation to maritime security level 1:

(a) the security measures, identified in the security assessment for the operation, for implementation at that level; and

(b) the measures that have been implemented; and

(c) a schedule for implementing the measures that have not been implemented; and

(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.

5A.165 Maritime security levels 2 and 3

An offshore security plan for an offshore service provider must set out, in relation to maritime security levels 2 and 3, the additional security measures that the service provider will implement if the Secretary declares that maritime security level 2 or 3 is in force for a port or airport at which the service provider operates.

5A.170 Declarations of security

An offshore security plan for an offshore service provider must provide for:

(a) the circumstances in which the service provider will request a declaration of security with another offshore industry participant or a ship; and

(b) the procedures for negotiating the security measures and responsibilities of the service provider and the participant in those circumstances; and

(c) how security measures identified in a declaration will be implemented to ensure compliance by the service provider and the participant with their security plans and with the declaration.

Replaced Authorised Version registered 19/04/2024 F2021C00921

5A.175 Protection of plan

An offshore service provider must ensure that the offshore security plan for the service provider is protected against unauthorised access, amendment and disclosure.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 6—Maritime security zones

Division 6.1—Preliminary

6.05 Access not to be denied

(1) Nothing in this Part has the effect of preventing entry into a maritime security zone by a person who:

(a) is accompanied by a law enforcement officer for the purposes of an investigation; or

(b) is an Australian Federal Police employee, a member of the Australian Federal Police, or an officer or employee of the police force or service of a State or Territory, who requires access for the purposes of a police investigation; or

(c) is otherwise authorised by a law of the Commonwealth, State or Territory to enter the maritime security zone.

Example: For paragraph (c), entry to maritime security zones must not be denied to law enforcement officers, customs officers or AMSA officers if the entry is required in the course of their duties.

(2) Nothing in this Part has the effect of preventing a member of the Australian Defence Force who is on duty:

(a) from entering a maritime security zone; or

(b) from taking into a maritime security zone vessels, vehicles or goods:

(i) for the purpose of gaining access to a ship that is under the control, or in the service, of the Australian Defence Force; or

(ii) in connection with the movement, loading, unloading, maintenance or provisioning of such a ship.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 6.1A—Control of maritime security zones

Subdivision 6.1A.1—Preliminary

6.07A Purpose of Division 6.1A

(1) This Division provides for a scheme under which:
  (a) an MSIC is issued to identify a person who has been the subject of a background check; and
  (b) a maritime industry participant must not allow a person to enter, or remain in, a maritime security zone unless the person:
    (i) is properly displaying a blue MSIC or a temporary MSIC; or
    (ii) is escorted by a person who is properly displaying a blue MSIC or a temporary MSIC; and
  (c) an issuing body must not allow a person to be directly involved in the issue of blue MSICs or white MSICs unless the person holds a blue MSIC or a white MSIC.

(2) The Division includes requirements about:
  (a) the display of MSICs; and
  (b) issuing bodies for MSICs; and
  (c) the issue of an MSIC to a person; and
  (d) the expiry, suspension and cancellation of MSICs; and
  (e) the issuing and display of temporary MSICs.

6.07B Definitions for Division 6.1A

(1) In this Division:

adverse criminal record, in relation to a person, has the meaning given by subregulation (3).

AFP means the Australian Federal Police established under the *Australian Federal Police Act 1979*.

ASIO means the Australian Security Intelligence Organisation established under the *Australian Security Intelligence Organisation Act 1979*.

AusCheck facility means a facility made available by the Secretary AGD for the purposes of the AusCheck scheme.

AusCheck scheme means the scheme prescribed for the purposes of section 8 of the *AusCheck Act 2007*.

background check, for an individual, means an assessment, under the AusCheck scheme, of information about any of the matters mentioned in section 5 of the *AusCheck Act 2007*.

Replaced Authorised Version registered 19/04/2024 F2021C00921

blue MSIC means a blue maritime security identification card, in a form approved under subregulation 6.08J(2), issued under this Division.

Category A identification document means:

(a) for a person who was born in Australia—either of the following:
  (i) the person's Australian birth certificate;
  (ii) a notice given to the person under section 37 of the *Australian Citizenship Act 2007*; or

(b) for any other person—a valid document that provides evidence of the start of the person's identity in Australia.

Example 1: An Australian naturalisation certificate.

Example 2: A visa entitling the person to enter Australia.

Example 3: A movement record made available to the person by the Immigration Department.

Category B identification document, for a person, means a current and valid document issued to the person by a Commonwealth, State or Territory Department or agency, or by a government of a foreign country or an agency of a government of a foreign country, that provides photographic proof of the person's identity and includes the person's signature.

Example 1: A driver's licence issued by the Commonwealth, a State or a Territory, or by a foreign government.

Example 2: An Australian or foreign passport.

Category C identification document, for a person, means a current and valid document that provides evidence of the person's use of identity while operating in the community (which may be a community outside Australia).

Example: A Medicare card, or a membership card issued by a private health insurer.

Category D identification document, for a person, means a valid document that provides evidence of the person's current residential address (which may be a residential address outside Australia) and is less than 6 months old.

Example: A utilities notice.

Commonwealth authority means:

(a) a Commonwealth department; or

(b) a body established for a public purpose by or under a law of the Commonwealth.

conviction (of a person for an offence) has the meaning given by subsection 85ZM(1) of the *Crimes Act 1914*, but does not include:

(a) a spent conviction (within the meaning given by subsection 85ZM(2) of that Act) if Division 3 of Part VIIC of that Act applies to the person; or

(b) a conviction for an offence of which, under a law relating to pardons or quashed convictions, the person is taken never to have been convicted.

Note 1: Under the definition of ***conviction*** in subsection 85ZM(1) of the *Crimes Act 1914*, a person is also taken to have been convicted of an offence if the person has been convicted of the offence but no conviction has been recorded, and if a court has taken

Replaced Authorised Version registered 19/04/2024 F2021C00921

the offence into account in sentencing the person for another offence (see paragraphs 85ZM(1)(b) and (c)).

Note 2: Under Part VIIC of the *Crimes Act 1914*, if a person receives a free and absolute pardon for an offence against a law of the Commonwealth or a Territory because the person was wrongly convicted of the offence, the person is taken for all purposes never to have been convicted (see section 85ZR).

Note 3: In certain circumstances, Division 3 of Part VIIC of the *Crimes Act 1914* ceases to apply to a person in relation to a spent conviction if Division 4 (Convictions of further offences) applies.

Note 4: Under the *Crimes Act 1914*, a person need not disclose convictions that:
(a) have been quashed (see section 85ZT); or
(b) are spent (see section 85ZV).

Note 5: Convictions for certain offences do not become spent for the purposes of assessing whether to issue the convicted person with an MSIC—see paragraph 85ZZH(k) of the *Crimes Act 1914* and Schedule 2 to the *Crimes Regulations 2019*.

directly involved in the issue of MSICs: a person is ***directly involved in the issue of MSICs*** if the person performs any of the following activities:

(a) accepting applications for MSICs;
(b) applying for background checks under this Division;
(ba) receiving documents given to an issuing body in person in accordance with this Division;
(c) verifying identification documents for the purposes of this Division;
(d) printing or producing MSICs;
(e) issuing MSICs, including considering whether criteria for the issue of MSICs are satisfied and whether MSICs are to be issued with conditions;
(f) storing equipment associated with the production of MSICs;
(g) destroying MSICs that are no longer required, including expired or cancelled MSICs.

exempt person, in relation to a maritime security zone, or a part of a maritime security zone, means a person who under the Act or these Regulations, is not required to properly display a valid MSIC in the zone or that part of the zone.

foreign official means any of the following:

(a) a member of the diplomatic staff (including the head) of a diplomatic mission established in Australia;
(b) a member of the consular staff (including the head) of a consular post established in Australia;
(c) any other member of the staff of such a diplomatic mission or consular post.

holder, of an MSIC or a temporary MSIC, means the person to whom it is issued.

identification document means any of the following:

(a) a Category A identification document;
(b) a Category B identification document;
(c) a Category C identification document;

Replaced Authorised Version registered 19/04/2024 F2021C00921

(d) a Category D identification document;
(e) any other document used to identify a person for the purposes of this Division.

imprisonment includes periodic detention, home-based detention and detention until the rising of a court, but does not include an obligation to perform community service.

issuing body means a person or body:
(a) that is authorised to issue MSICs; or
(b) that is a transitional issuing body.

maritime-security-relevant offence means an offence mentioned in an item of a table in Schedule 1 against a law of:
(a) the Commonwealth, a State or Territory; or
(b) a foreign country or part of a foreign country.

MSIC means a blue MSIC or a white MSIC.

MSIC applicant means a person who has applied for the issue of an MSIC in accordance with regulation 6.08B.

MSIC plan, for an issuing body, means a plan of the kind described in regulation 6.07Q, and includes a plan of that kind as varied under regulation 6.07S or 6.07T.

qualified security assessment has the meaning given by subsection 35(1) of the *Australian Security Intelligence Organisation Act 1979*.

Secretary AGD means the Secretary who is responsible for administering the AusCheck scheme.

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

sentence includes a suspended sentence.

temporary MSIC means an identity document issued under regulation 6.08K.

tier 1 offence means a maritime-security-relevant offence mentioned in the table in clause 1 of Schedule 1.

tier 2 offence means a maritime-security-relevant offence mentioned in the table in clause 2 of Schedule 1.

tier 3 offence means a maritime-security-relevant offence mentioned in the table in clause 3 of Schedule 1.

transitional issuing body means a body declared by the Secretary under subregulation 6.07ZB(1) to be a transitional issuing body.

white MSIC means a white maritime security identification card, in a form approved under subregulation 6.08J(3), issued under this Division.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) For this Division, a person's security assessment is ***adverse*** if there is an adverse security assessment within the meaning of subsection 35(1) of the *Australian Security Intelligence Organisation Act 1979* for the person.

(3) A person has an ***adverse criminal record*** if the person:
  (a) has been convicted of a tier 1 offence or a tier 2 offence; or
  (b) has been convicted of, and sentenced to imprisonment for, a tier 3 offence.

6.07D Meaning of valid blue MSIC or valid temporary MSIC

(1) For this Division, a blue MSIC or a temporary MSIC is ***valid*** if:
  (a) it is issued in accordance with this Division; and
  (b) it is not expired, suspended or cancelled; and
  (c) it is not altered or defaced (permanently or temporarily); and
  (d) the person who shows or displays it is the person to whom it was issued.

(3) A temporary MSIC is valid only in the maritime security zone or zones that, under subparagraph 6.08KA(1)(c)(v), the temporary MSIC displays or includes.

6.07E Meaning of *properly displaying*

(1) For this Division, a person is ***properly displaying*** an MSIC only if:
  (a) the person is wearing the MSIC as required by this regulation; and
  (b) the whole of the front of the MSIC is clearly visible at all times that it is being worn.

(2) The person must wear the MSIC in 1 of the following ways:
  (a) attached, at or above the waist, to the front or side of his or her clothing;
  (b) on a band around his or her upper arm.

(3) In this regulation, ***MSIC*** means a blue MSIC or a temporary MSIC, but does not include a white MSIC.

Note: A requirement under these Regulations to display a valid MSIC cannot be satisfied with a white MSIC.

6.07F Meaning of *operational need*

(1) For the purposes of this Division, a person has an ***operational need*** to hold a blue MSIC if his or her occupation or business interests require, or will require, him or her to have unmonitored access to a maritime security zone at least once each year.

(2) For the purposes of this Division, a person has an ***operational need*** to hold a white MSIC if:
  (a) the person is required to be directly involved in the issue of MSICs for an issuing body; or
  (b) the person is an employee of a Commonwealth agency who is required to be directly involved in making decisions relating to the issuing of MSICs; or

Replaced Authorised Version registered 19/04/2024 F2021C00921

(c) the person is a foreign official who requires access to a maritime security zone for the purposes of the foreign official's official duties.

6.07H Authentication of certain foreign documents

(1) In this regulation:

Hague Convention means the *Convention Abolishing the Requirement of Legalisation for Foreign Public Documents*, done at the Hague on 5 October 1961.

(2) This regulation applies if a person presents to an issuing body, as an identification document, a document that is a public document for the purposes of the Hague Convention and was issued in a country (other than Australia) that is a Contracting State to that Convention.

(3) The body may require the person to have the authenticity of the document certified in accordance with that Convention.

Note: The authentication procedure involves the endorsement on, or attachment to, the document of a certificate in a standard form. Details of the procedure and any fee payable should be available from the embassy of the country in which the document was issued.

6.07HA Identification documents not in English must be translated

(1) This regulation applies if a person gives an issuing body, as an identification document, a document that is not in English.

(2) The person must also give the issuing body an original or certified copy of an accurate translation of the document into English.

Subdivision 6.1A.2—Display of MSICs

6.07I Definitions for Subdivision 6.1A.2

In this Subdivision:

escort means a person who escorts, or continuously monitors, another person in a maritime security zone.

Note: Unless exempt, an escort must hold a valid MSIC or valid temporary MSIC: see regulation 6.07J.

visitor, to a maritime security zone, means a person who is entitled to be in the zone because he or she is being escorted or continuously monitored.

6.07J Requirement to display MSIC in maritime security zones

(1) A person commits an offence if:
(a) he or she is in a maritime security zone; and
(b) he or she fails to properly display a valid blue MSIC or valid temporary MSIC.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Penalty:

(c) for a first offence—5 penalty units; or

(d) for a second offence within 2 years of an offence—10 penalty units; or

(e) for a third or subsequent offence within 2 years of an offence—20 penalty units.

(2) Subregulation (1) does not apply to:

(a) a visitor to the zone, if his or her escort:

(i) is displaying a valid blue MSIC or valid temporary MSIC; or

(ii) is carrying a valid blue MSIC but, under regulation 6.07M, is exempt from the requirement to display it; or

(iii) is exempt, under regulation 6.07M, from the requirement to carry a valid blue MSIC; or

(iv) is a person to whom paragraph (f) applies; or

(b) the holder of an identification document issued by an arm of the Defence Force who:

(i) is displaying his or her identification document; and

(ii) is in the zone as part of his or her duties for the Force; or

(c) a person who is in a private living area of a security regulated offshore facility; or

(d) a person who, with the permission of the ship's master, is on board a security regulated ship that is in a water-side restricted zone; or

(e) a person who:

(i) is a crew member of a security regulated ship that is in a water-side restricted zone and docked at a land-side restricted zone; and

(ii) is in the land-side restricted zone, carrying out his or her duties as a crew member; and

(iii) does not enter a maritime security zone other than a zone mentioned in subparagraph (i); or

(f) a person who:

(i) is a crew member of an offshore facility that is in an offshore security zone; and

(ii) is in the offshore security zone, carrying out his or her duties as such a crew member; and

(iii) holds a valid blue MSIC; or

(g) a person who:

(i) is a crew member of a regulated foreign ship, or a foreign ship regulated as an offshore facility, that is in an offshore water-side zone; and

(ii) is in the offshore water-side zone, carrying out his or her duties as such a crew member; and

(iii) is not an Australian citizen and does not hold a visa entitling him or her to work in Australia.

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

Replaced Authorised Version registered 19/04/2024 F2021C00921

(3) A contravention of subregulation (1) is an offence of strict liability.

(4) Subregulation (1) does not apply before 1 January 2007.

6.07K Person given disqualifying notice not to enter maritime security zone

(1) A person who has been given a disqualifying notice by the Secretary, or Secretary AGD, under regulation 6.08D must not enter a maritime security zone.

Penalty: 5 penalty units.

(2) Subregulation (1) does not apply to a person who is a visitor to a zone for the purpose of boarding or leaving a vessel:
(a) as part of a recreational activity; or
(b) as a passenger.

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) A contravention of subregulation (1) is an offence of strict liability.

6.07L Offence—failure to properly escort visitor

(1) An escort is guilty of an offence if he or she fails to escort, or continuously monitor, a visitor in accordance with the procedures set out in the maritime security plan, ship security plan or offshore security plan of the maritime industry participant concerned.

Penalty: 5 penalty units.

(2) A contravention of subregulation (1) is an offence of strict liability.

6.07M Persons exempted by Secretary from requirement to hold, carry or display MSIC

(1) Despite regulation 6.07J, somebody to whom the Secretary has given an exemption under this regulation need not display an MSIC in a maritime security zone.

(2) Within 30 days after receiving an application, the Secretary must:
(a) give or refuse the exemption; and
(b) notify the person in writing of the decision and, if the decision is a refusal, the reasons for it.

(3) On the Secretary's own initiative, or on written application by a person, the Secretary may give a person, or all persons in a specified class, exemption from the requirement, in 1 or more specified maritime security zones, to:
(a) hold an MSIC; or
(b) carry an MSIC; or
(c) display an MSIC.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(4) Before giving or refusing an exemption, the Secretary must consider:
  (a) why the exemption is necessary; and
  (b) the likely effect of the proposed exemption on the security of maritime transport or an offshore facility in the zone; and
  (c) how long the proposed exemption will last, if it is given; and
  (d) anything else relevant that the Secretary knows about.

(5) The Secretary may give an exemption:
  (a) for a particular period and subject to a condition or conditions mentioned in the exemption; or
  (b) limited to a particular zone or part of a zone.

(6) If the Secretary gives an exemption to all persons in a specified class, the Secretary must publish a notice of the exemption in the *Gazette*.

(7) In this regulation, ***MSIC*** means a blue MSIC or a temporary MSIC, but does not include a white MSIC.

6.07N Access by emergency personnel

(1) Nothing in this Division requires or authorises a maritime industry participant to prevent any of the following having access to any part of a maritime security zone:
  (a) members of the Defence Force who are responding to an event or threat of unlawful interference with maritime transport or an offshore facility;
  (b) law enforcement officers or ambulance, rescue or fire service officers who are responding to an emergency.

(2) A requirement of this Part to hold, carry or display an MSIC or a temporary MSIC does not apply to a person referred to in paragraph (1)(a) or (b).

Subdivision 6.1A.3—MSIC issuing bodies

6.07O Application for authorisation to issue MSICs

(1) The following may apply, in writing, to the Secretary for authorisation as an issuing body:
  (a) a maritime industry participant;
  (b) a body representing participants;
  (c) a body representing employees of participants;
  (d) a Commonwealth authority;
  (e) the Comptroller-General of Customs (within the meaning of the *Customs Act 1901*).

  Note: Knowingly making a false or misleading statement in an application is an offence punishable by imprisonment for 12 months—see the *Criminal Code*, section 136.1.

(2) However, a participant may engage an agent to issue MSICs and the agent may apply to be an issuing body.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(3) An application must be accompanied by a statement setting out the applicant's proposed MSIC plan.

(4) An applicant is entitled to perform the functions or exercise the powers of an issuing body only if the applicant's MSIC plan is approved by the Secretary.

6.07P Decision on application

(1) If the Secretary needs more information to deal with an application under regulation 6.07O, the Secretary may ask the applicant, in writing, to provide the information.

(2) Before the end of 30 days after receiving an application (or, if the Secretary asks for more information under subregulation (1), before the end of 30 days after receiving the information), the Secretary must:
  (a) approve, or refuse to approve, the applicant's proposed MSIC plan; and
  (b) authorise, or refuse to authorise, the applicant as an issuing body; and
  (c) notify the body in writing of the decision and, if the decision is a refusal, the reasons for the decision.

Note: Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the decision reviewed.

(3) If the Secretary has not authorised, or refused to authorise the applicant as an issuing body within the period allowed by subregulation (2), the Secretary is taken to have refused to authorise the applicant as an issuing body.

(4) The Secretary must not authorise the applicant as an issuing body unless the Secretary is satisfied that:
  (a) the applicant's proposed MSIC plan adequately addresses the matters mentioned in subregulation 6.07Q(2); and
  (b) authorising the applicant as an issuing body would not be likely to be a threat to the security of maritime transport or an offshore facility.

(5) The Secretary may authorise an applicant as an issuing body subject to a condition set out in the instrument of authorisation.

6.07Q What an MSIC plan is

(1) An ***MSIC plan*** for an issuing body sets out the procedures to be followed by the issuing body in the performance of its functions under this Division, and the exercise of its powers under this Division.

Note: An applicant for authorisation as an issuing body must provide with its application a statement of its proposed MSIC plan (see regulation 6.07O).

(2) The MSIC plan must include procedures in relation to the following matters:
  (a) accepting applications for MSICs;
  (b) applying for background checks under this Division;
  (c) verifying identification documents for the purposes of this Division;

Replaced Authorised Version registered 19/04/2024 F2021C00921

(d) determining whether MSIC applicants have an operational need for an MSIC;
(e) printing and producing MSICs;
(f) issuing MSICs, including considering whether criteria for the issue of MSICs are satisfied and whether MSICs are to be issued with conditions;
(g) distributing MSICs to applicants;
(h) ensuring that holders of MSICs are aware of obligations that apply in relation to holding MSICs;
(i) storing and transporting MSICs;
(j) collecting, storing and destroying information and documents about MSICs and MSIC applications;
(k) storing equipment associated with the production of MSICs;
(l) taking all reasonable steps to recover blue MSICs that are no longer required, including expired or cancelled blue MSICs;
(m) destroying blue MSICs that are no longer required, including expired or cancelled blue MSICs;
(n) cancelling access control arrangements that are related to blue MSICs that are no longer required, including expired or cancelled blue MSICs, and blue MSICs that have been lost, stolen or destroyed;
(o) keeping records of the activities of the issuing body;
(p) if the issuing body proposes to engage other entities to perform activities on its behalf—engaging such other entities to perform such activities;
(q) conducting an ongoing quality assurance process of the procedures in the plan and the implementation of the procedures;
(r) conducting an annual audit of the procedures in the plan and the implementation of the procedures;
(s) the issuing body ceasing to be an issuing body, including procedures to ensure that information about applications for MSICs, and holders of MSICs, is appropriately handled or preserved.

(3) The procedures must be such as to ensure that the issuing body performs its functions under this Division, and exercises its powers under this Division, in an appropriately secure manner.

(4) The MSIC plan must be accompanied by a document that sets out the following details:
(a) the issuing body's name;
(b) the issuing body's ABN, ACN or ARBN (if any);
(c) if the issuing body is a body corporate—the name of its chief executive officer or manager;
(d) the issuing body's postal address;
(e) the issuing body's physical address (if different from the issuing body's postal address);
(f) the issuing body's email address;
(g) the contact telephone number for the issuing body, including an after-hours number;

Replaced Authorised Version registered 19/04/2024 F2021C00921

(h) an alternative contact person and number.

(5) An issuing body commits an offence of strict liability if:
(a) the issuing body becomes aware of a change in a detail referred to in subregulation (4); and
(b) the issuing body does not, within 5 working days after becoming aware of the change, notify the Secretary in writing of the detail as changed.

Penalty: 20 penalty units.

6.07R Issuing body to give effect to MSIC plan

(1) An issuing body must not fail to give effect to its MSIC plan.

Penalty: 50 penalty units.

(2) Without limiting subregulation (1), an issuing body fails to give effect to its MSIC plan if it:
(a) fails to do something that its MSIC plan requires that it do; or
(b) does something that its MSIC plan requires that it not do; or
(c) does something that its MSIC plan requires that it do, but does so in a way that contravenes the plan.

(3) A contravention of subregulation (1) is an offence of strict liability.

(4) However, an issuing body may apply, in writing, to the Secretary for exemption from giving effect to its MSIC plan in a particular case or respect.

(5) If the Secretary needs more information to deal with an application, the Secretary may ask the applicant, in writing, to provide the information.

(6) Within 30 days after receiving an application (or, if the Secretary asks for more information under subregulation (5), within 30 days after receiving the information), the Secretary must:
(a) grant or refuse the exemption; and
(b) notify the body in writing of the decision and, if the decision is a refusal, the reasons for the decision.

Note: Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the decision reviewed.

(7) If the Secretary has not approved, or refused to approve, the exemption within the period allowed by subregulation (6), the Secretary is taken to have refused to approve the exemption.

(8) The Secretary may also grant, on his or her own initiative, an issuing body a written exemption from giving effect to its MSIC plan in a particular case or respect.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(9) Before granting or refusing an exemption under this regulation, the Secretary must consider:
  (a) the justification for the proposed exemption; and
  (b) the likely effect of the proposed exemption on each of the matters mentioned in subregulation 6.07Q(2); and
  (c) how long the proposed exemption will be for, if it is granted; and
  (d) anything else relevant that the Secretary knows about.

(10) The Secretary may grant an exemption for a particular period and subject to a condition mentioned in the exemption.

6.07S Direction to vary MSIC plan

(1) If the Secretary is satisfied that an issuing body's MSIC plan does not adequately address a matter mentioned in subregulation 6.07Q(2), the Secretary may direct the body, in writing, to vary the plan.

(2) However, the Secretary must not give a direction under subregulation (1) unless the Secretary is satisfied that the plan, as varied, would adequately address the relevant matter mentioned in subregulation 6.07Q(2).

(3) A direction must:
  (a) indicate the variation needed; and
  (b) state the time within which the issuing body must submit an appropriately varied plan to the Secretary.

(4) An issuing body must comply with such a direction.

Note: Regulation 6.07W provides for the revocation of the authorisation of a body that does not comply with a direction.

6.07T Variation of MSIC plan by issuing body

(1) An issuing body may:
  (a) review its MSIC plan at any time; and
  (b) submit a written proposed variation of the plan to the Secretary for approval.

(2) If the Secretary needs more information to deal with a proposed variation, the Secretary may ask the body, in writing, to provide the information.

(3) Before the end of 30 days after receiving the proposed variation (or, if the Secretary asks for more information under subregulation (2)), before the end of 30 days after receiving the information), the Secretary must:
  (a) approve or refuse to approve the variation; and
  (b) notify the body in writing of the decision and, if the decision is a refusal, the reasons for the decision.

Note: Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the

Replaced Authorised Version registered 19/04/2024 F2021C00921

decision notice of the making of the decision and of the person's right to have the decision reviewed.

(4) If the Secretary has not approved, or refused to approve, the variation within the period allowed by subregulation (3), the Secretary is taken to have refused to approve the variation.

(5) The Secretary must approve the variation if the plan, as varied, will adequately address the matters mentioned in subregulation 6.07Q(2).

6.07U Inspection of issuing bodies' MSIC plan and records

(1) An issuing body must:
  (a) keep a copy of its MSIC plan or any variation to the plan for at least 7 years after the day on which the plan is approved or varied; and
  (b) keep any record relating to how the body gives effect to its MSIC plan for at least 7 years after the day on which it is made.

(2) An issuing body must allow a maritime security inspector to inspect the plan and records kept for subregulation (1) on request, subject to reasonable notice.

6.07V Issuing bodies' staff

(1) An issuing body other than a Commonwealth authority must not allow a person to be directly involved in the issue of MSICs unless he or she holds an MSIC.

Penalty: 20 penalty units.

(2) A Commonwealth authority that is an issuing body must not allow a person to be directly involved in the issue of MSICs unless he or she holds an MSIC.

6.07W Revocation of authorisation for cause

(1) The Secretary must revoke an issuing body's authorisation as an issuing body if, in the opinion of the Secretary:
  (a) the body's MSIC plan does not adequately address a matter mentioned in subregulation 6.07Q(2) and it is unlikely that a direction under regulation 6.07S will make the plan adequately address the matter; or
  (b) allowing the body's authorisation to continue would be likely to be a significant threat to the security of maritime transport or an offshore facility; or
  (c) the body does not comply with a direction of the Secretary under regulation 6.07S.

(2) The Secretary may revoke the authorisation of an issuing body if the body contravenes:
  (a) this Division; or
  (b) a condition of its authorisation; or
  (c) its MSIC plan.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(3) In making a decision under subregulation (2), the Secretary must consider:
  (a) the kind and seriousness of the contravention; and
  (b) whether the issuing body has previously contravened this Division, a condition of its authorisation or its MSIC plan.

(4) As soon as practicable after revoking the authorisation of a body under this regulation, the Secretary must notify the body in writing of the revocation and the reasons for the revocation.

  Note: Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the decision reviewed.

(5) The revocation takes effect when written notice of the revocation is given to the body.

6.07X Secretary's discretion to revoke authorisation

(1) The Secretary may revoke the authorisation of a body (the ***relevant body***) as an issuing body:
  (a) on the Secretary's own initiative; or
  (b) on application by the relevant body under regulation 6.07Y.

(2) If the Secretary is considering revoking the authorisation of the relevant body under this regulation on the Secretary's own initiative, the Secretary must give the relevant body written notice inviting the relevant body to respond within 14 days.

(3) Before deciding whether to revoke the authorisation under this regulation, the Secretary must consider the following matters:
  (a) the number of MSICs issued by the relevant body that:
    (i) are in effect; or
    (ii) are suspended under regulation 6.08LF; or
    (iii) have been cancelled or have expired, but may be reinstated; or
    (iv) have been cancelled or have expired, if another MSIC may be issued to the former holder without a further background check being conducted;
  (b) whether there are any applications for MSICs that the relevant body is yet to approve or refuse to approve;
  (c) whether there is another issuing body that can be the issuing body for:
    (i) the MSICs issued by the relevant body; and
    (ii) any applications referred to in paragraph (b);
  (d) whether the relevant body should be a transitional issuing body under regulation 6.07ZB;
  (e) any information given to the Secretary by the Secretary AGD about the following:
    (i) any applications referred to in paragraph (b);

Replaced Authorised Version registered 19/04/2024 F2021C00921

(ii) any applications for MSICs that have been approved by the relevant body, but the MSIC has not yet been issued;

(iii) the effect the revocation of the body's authorisation may have on operations;

(f) if the relevant body has responded to a notice under subregulation (2)—the relevant body's response, including whether the relevant body wants to continue to be an issuing body;

(g) any other matter the Secretary considers relevant.

(4) If the Secretary decides to revoke, or refuse to revoke, the relevant body's authorisation under this regulation, the Secretary must give the body written notice of the Secretary's decision and the reasons for the decision.

Note: If the body applied for the revocation, the Secretary must make the decision and give the body written notice within 30 days of receiving the application—see subregulation 6.07Y(2).

(5) If the Secretary decides to revoke the relevant body's authorisation under this regulation, and there are:

(a) MSICs referred to in paragraph (3)(a) issued by the relevant body; or

(b) applications for MSICs that the relevant body is yet to approve or refuse to approve;

the Secretary must do one of the following:

(c) decide, under regulation 6.07ZA, that another issuing body is to be the issuing body for the MSICs and applications;

(d) declare the relevant body to be a transitional issuing body under regulation 6.07ZB and postpone the revocation until the time referred to in paragraph 6.07ZB(2)(c).

Note: If there are no MSICs or applications referred to in paragraph (a) or (b), the Secretary may revoke the relevant body's authorisation without doing the things in paragraph (c) or (d).

(6) In deciding, for the purposes of subregulation (5), which of paragraphs (5)(c) and (d) is to apply, the Secretary must consider the matters referred to in paragraphs (3)(a), (b), (c), (d), (f) and (g).

(7) A revocation of the relevant body's authorisation under this regulation takes effect:

(a) if the Secretary declares the relevant body to be a transitional issuing body under regulation 6.07ZB—at the time referred to in paragraph 6.07ZB(2)(c); or

(b) otherwise—at the time the Secretary decides to revoke the authorisation.

(8) The Secretary must tell the Secretary AGD if the Secretary decides to revoke the relevant body's authorisation under this regulation.

6.07Y Application by issuing body for revocation of authorisation

(1) An issuing body may apply, in writing, for the Secretary to revoke under regulation 6.07X the authorisation of the body as an issuing body.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) Within 30 days after receiving the written application, the Secretary must:
  (a) decide to revoke, or refuse to revoke, the applicant's authorisation as an issuing body; and
  (b) give the applicant written notice under subregulation 6.07X(4).

Note: If the Secretary decides to revoke the applicant's authorisation as an issuing body and there are MSICs or applications referred to in paragraph 6.07X(5)(a) or (b), the Secretary must also make a decision referred to in paragraph 6.07X(5)(c) or (d).

(3) If the Secretary does not make a decision about an application within the 30 days referred to in subregulation (2), the Secretary is taken to have refused to revoke the applicant's authorisation at the end of that period.

6.07Z Revocation does not prevent another application for authorisation

The revocation of a body's authorisation as an issuing body under regulation 6.07W or 6.07X does not prevent the body applying for a new authorisation under regulation 6.07O.

6.07ZA Responsibility for MSICs, applications and records if body ceases to be an issuing body

(1) This regulation applies in relation to a body (the ***original issuing body***) that was an issuing body if:
  (a) the Secretary revokes the authorisation of the body as an issuing body under regulation 6.07W or 6.07X; or
  (b) the body ceases to exist; or
  (c) for any other reason, the body no longer performs the functions or exercises the powers of an issuing body.

(2) The Secretary may decide that another issuing body (the ***new issuing body***) is to be the issuing body for:
  (a) any MSICs (***transferred MSICs***) issued by the original issuing body that:
    (i) are in effect; or
    (ii) are suspended under regulation 6.08LF; or
    (iii) have been cancelled or have expired, but may be reinstated; or
    (iv) have been cancelled or have expired, if another MSIC may be issued to the former holder without a further background check being conducted; and
  (b) any applications for MSICs (***transferred MSIC applications***) made to the original issuing body in relation to which the original issuing body:
    (i) has applied to the Secretary AGD for a background check (whether or not the background check has been completed); but
    (ii) has not yet issued, or refused to issue, an MSIC.

(3) The Secretary must tell the Secretary AGD who the new issuing body for the transferred MSICs and transferred MSIC applications will be.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Transferred MSICs and transferred MSIC applications

(4) A transferred MSIC is not affected by the original issuing body no longer being an issuing body.

(5) The new issuing body is not responsible for the actions of the original issuing body in relation to a transferred MSIC.

(6) The new issuing body may continue to deal with a transferred MSIC application as if it had been made to the new issuing body, and if the new issuing body does so:

(a) subject to paragraph (b), anything done by or in relation to the original issuing body in relation to the transferred MSIC application is taken, for the purposes of the new issuing body dealing with the application under this Division, to have been done by or in relation to the new issuing body; but

(b) the new issuing body may disregard anything done by or in relation to the original issuing body in relation to the transferred MSIC application for the purposes of dealing with the application under this Division, if the new issuing body considers it appropriate to do so.

Note: For example, the new issuing body may continue to process a transferred MSIC application, and may issue the MSIC applied for, in reliance on identification documents provided to the original issuing body. However, the new issuing body may choose not to rely on the documents, and may require the applicant to provide identification documents again, if the new issuing body considers it appropriate to do so.

Transfer of records and documents to new issuing body

(7) The original issuing body must transfer to the new issuing body:

(a) the original issuing body's register of MSICs, to the extent that the register relates to transferred MSICs; and

(b) any records or documents (including records or documents containing AusCheck scheme personal information within the meaning of the *AusCheck Act 2007*) in the original issuing body's possession that relate to:

(i) transferred MSICs; or

(ii) transferred MSIC applications.

Transfer of records and documents to Secretary

(8) The original issuing body must transfer to the Secretary any records or documents (including records or documents containing AusCheck scheme personal information within the meaning of the *AusCheck Act 2007*) that subregulation 6.08U(2) requires the original issuing body to retain, other than records or documents transferred to a new issuing body (if any) under subregulation (7) of this regulation.

Note: Subregulation (8) applies whether or not there is a new issuing body.

Replaced Authorised Version registered 19/04/2024 F2021C00921

6.07ZB Transitional issuing bodies

(1) The Secretary may, in writing, declare an issuing body to be a transitional issuing body.

(2) If the Secretary declares an issuing body to be a transitional issuing body, the following apply to the body:

(a) beginning on the day after the Secretary makes the declaration, the transitional issuing body:

(i) must not issue a new MSIC unless the issuing body received the application for the MSIC before the issuing body was declared to be a transitional issuing body; and

(ii) must not apply to the Secretary AGD for a background check, other than under regulation 6.08LBA;

(b) the transitional issuing body continues to be the issuing body for any MSICs issued by the issuing body, and may issue replacement MSICs;

(c) the transitional issuing body's authorisation as an issuing body is taken to be revoked immediately after the expiry or cancellation of the last MSIC issued by the body.

Note: A transitional issuing body remains an issuing body (see the definition of ***issuing body*** in subregulation 6.07B(1)).

(3) The Secretary must tell the Secretary AGD if the Secretary declares a body to be a transitional issuing body.

Offence

(4) A person commits an offence if:

(a) the person is a transitional issuing body; and

(b) the person issues an MSIC, a card resembling an MSIC, or a card apparently intended to be taken to be an MSIC; and

(c) the MSIC or card:

(i) is not a replacement MSIC; and

(ii) is not a new MSIC that was applied for before the person was declared to be a transitional issuing body.

Penalty: 50 penalty units.

Subdivision 6.1A.4—MSICs: issue, expiry, suspension and cancellation

6.08B MSICs—application

(1) A person may, in writing, apply to an issuing body for a blue MSIC or a white MSIC.

(2) An applicant for a blue MSIC must state in the application whether the person is applying for a blue MSIC that is to be in force for 2 years or 4 years.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Note: A blue MSIC issued to a person on the basis of being a person mentioned in subparagraph 6.08C(1)(c)(iii), or a white MSIC, may be in force for only 2 years: see regulation 6.08I.

6.08BA Application for background check

An issuing body may apply to the Secretary AGD for a background check on:

(a) an applicant for an MSIC; or

(b) the holder of an MSIC if the issuing body considers on reasonable grounds that either or both of the following subparagraphs apply in relation to the last application (the ***previous application***) for a background check on the holder made under paragraph (a) or (c):

(i) any of the requirements of the *AusCheck Regulations 2017* for the previous application were not satisfied;

(ii) the Secretary AGD did not have all of the required information (within the meaning of the *AusCheck Regulations 2017*) for the individual when AusCheck undertook a background check in response to the previous application; or

(c) the holder of an MSIC who has notified the issuing body under regulation 6.08LB that the holder has been convicted of and sentenced for a maritime-security-relevant offence.

6.08BB Requirements for verifying identity

(1) This regulation sets out how a person's identity is to be verified by an issuing body for the purposes of paragraph 6.08C(1)(b).

(2) The person must:

(a) subject to subregulation (3), give to the issuing body, in person, an original of each of the following for the person:

(i) a Category A identification document;

(ii) a Category B identification document that is different from the Category A identification document;

(iii) a Category C identification document that is different from the Category A identification document and the Category B identification document;

(iv) if evidence of residential address is not set out in a document already given—a Category D identification document; and

(b) give to the issuing body the information required under the *AusCheck Regulations 2017* to be included in an application for a background check in relation to the person.

(3) If the Secretary has given an approval under regulation 6.08BC for alternative identification requirements to apply to the person, or a class of persons including the person, in relation to a requirement (the ***primary requirement***) referred to in paragraph (2)(a) of this regulation, the person may satisfy the primary requirement by complying with the alternative identification requirements.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(4) The issuing body must verify the person's identity at the time the person gives the documents referred to in paragraph (2)(a) (or any other documents given in accordance with alternative identification requirements) to the issuing body.

(5) To avoid doubt, the person must give the documents referred to in paragraph (2)(a) (or any other documents given in accordance with alternative identification requirements) to the issuing body even if the person has previously given the same documents to the same issuing body in relation to another application for the issue of an MSIC.

6.08BC Alternative requirements for verifying identity

Alternative identification requirements—persons

(1) If a person cannot satisfy one or more requirements to give a document to an issuing body under paragraph 6.08BB(2)(a), the issuing body may apply to the Secretary for approval of alternative identification requirements in relation to those requirements for the person.

(2) The application must:
  (a) be in writing; and
  (b) state whether the document or documents are one or more of the following:
    (i) a Category A identification document;
    (ii) a Category B identification document;
    (iii) a Category C identification document;
    (iv) a Category D identification document; and
  (c) state the reason why the person cannot satisfy the requirement or requirements; and
  (d) set out alternative identification requirements; and
  (e) if the alternative identification requirements relate to another document or other documents—include a copy of that document or those documents; and
  (f) include any other information that may assist the Secretary in making a decision about whether to approve the alternative identification requirements.

(3) In making a decision to approve, or refuse to approve, alternative identification requirements, the Secretary must consider the following matters:
  (a) the extent to which the issuing body can show evidence of the identity of the person;
  (b) the reason why the person cannot satisfy the requirement or requirements;
  (c) whether the alternative identification requirements proposed are sufficient to enable the Secretary AGD to conduct a background check.

(4) If the Secretary requires further information to consider the application, the Secretary may request the issuing body to give the further information.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(5) The Secretary must, in writing and within 30 days after receiving the application or, if further information is requested, within 30 days after receiving the further information:

(a) approve, or refuse to approve, the alternative identification requirements for the person; and

(b) notify the issuing body of the decision; and

(c) if the decision is a refusal—notify the issuing body of the reasons for the refusal.

Note: See section 27A of the *Administrative Appeals Tribunal Act 1975* for the requirements for a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the decision reviewed.

(6) If the Secretary has not made a decision on the application within the period mentioned in subregulation (5), the Secretary is taken to have refused to approve the application.

Alternative identification requirements—classes of persons

(7) If the Secretary is satisfied that a class of persons may be unable to meet one or more requirements under paragraph 6.08BB(2)(a), the Secretary may approve alternative identification requirements in relation to those requirements for the class of persons.

6.08C MSICs—issue

(1) An issuing body may issue an MSIC to a person if the following criteria are satisfied:

(a) the person has an operational need to hold an MSIC;

(b) the issuing body is satisfied of the person's identity, after verifying the person's identity in accordance with regulation 6.08BB;

(c) one of the following applies:

(i) the person has shown the issuing body a document that is evidence that he or she is an Australian citizen (for example, the person's Australian birth certificate or Australian passport or a notice given to the person under section 37 of the *Australian Citizenship Act 2007*);

(ii) the issuing body is satisfied that the person holds a visa entitling him or her to work in Australia;

(iii) the issuing body is satisfied that the person is a crew member of a regulated Australian ship that is registered in the Australian International Shipping Register under the *Shipping Registration Act 1981*;

(d) the issuing body has been notified in writing that a security assessment of the person has been made, and:

(i) the assessment was not adverse; or

(ii) if the assessment was qualified—the issuing body has received a notice from the Secretary that an MSIC may be issued because the

Replaced Authorised Version registered 19/04/2024 F2021C00921

person is not a threat to the security of maritime transport or an offshore facility;

(e) the issuing body has been notified in writing that a criminal history check of the person has been made, and:

(i) the check shows that the person does not have an adverse criminal record; or

(ii) if the check shows that the person has an adverse criminal record—the Secretary has approved an application to issue an MSIC to the person under paragraph 6.08F(3)(a).

(2) An issuing body commits an offence if:

(a) the issuing body issues an MSIC to a person; and

(b) the criteria for the issue of an MSIC mentioned in subregulation (1) are not satisfied.

Penalty: 50 penalty units.

(3) An offence against subregulation (2) is an offence of strict liability.

(4) However, if a person is younger than 18, the issuing body may issue an MSIC to the person if:

(a) the person meets the criteria in paragraphs (1)(a), (b), (c) and (d); and

(b) in the case of a person who was under 14 at the time the application for the MSIC was made—the application was accompanied by a written consent, given by a parent or guardian of the person, for the issuing body to perform its functions, and exercise its powers, in relation to the issuing of the MSIC (including by applying for a background check of the person).

Note: See paragraph 6.08I(2)(a) for when an MSIC issued under this subregulation ceases to be valid.

(5) Despite subregulation (2), the issuing body may issue an MSIC to a person if:

(a) the person's MSIC is cancelled under paragraph 6.08M(1)(f) or (g) or regulation 6.08N; and

(b) within 12 months after the cancellation:

(i) the person has an operational need to hold an MSIC; and

(ii) the person gives an issuing body a statutory declaration stating that, since the cancellation, no relevant circumstance of the person has changed; and

(iii) the issuing body lodges a request for the issue of an MSIC using the AusCheck facility.

(6) An issuing body may issue an MSIC subject to a condition, but must notify the holder in writing what the condition is.

(7) An issuing body may issue MSICs only in accordance with its MSIC plan.

Replaced Authorised Version registered 19/04/2024 F2021C00921

6.08CA AusCheck facility to be used when issuing MSIC

An issuing body issuing an MSIC under regulation 6.08C, 6.08E, 6.08F or 6.08L must use the AusCheck facility.

Penalty: 10 penalty units.

6.08D Issue of disqualifying notice

(1) This regulation applies if the background check of an applicant for an MSIC reveals that:
  (a) he or she has been convicted of a tier 1 offence; or
  (b) the security assessment of the person is adverse and is not a qualified security assessment.

(2) The Secretary AGD must send the person a notice in writing (a ***disqualifying notice***) that informs the person about the results of the background check and the effect of regulation 6.07K in relation to the person.

(2A) The Secretary AGD must give the Secretary a copy of a notice issued under subregulation (2).

(3) If the Secretary thinks it is necessary to do so to prevent unlawful interference with maritime transport or offshore facilities, or to prevent the use of maritime transport or offshore facilities in connection with serious crime, he or she may:
  (a) direct the issuing body to which the person applied for the issue of an MSIC, in writing, to give the Secretary the following information:
    (i) the name of the person's employer;
    (ii) the kind of business that the employer is engaged in; and
  (b) give a written notice to the person's employer, a maritime industry participant or both:
    (i) stating that, following a background check, a disqualifying notice has been sent to the person; and
    (ii) stating the information provided by the issuing body following a direction under paragraph (a).

6.08E Issue of MSICs to ASIC holders

An issuing body may issue an MSIC to a person without verifying that the person has satisfied the criteria set out in subregulation 6.08C(1) if the person:
  (a) holds an ASIC issued under the *Aviation Transport Security Regulations 2005*; and
  (b) has an operational need for the MSIC.

Note: The MSIC expires on the same day as the ASIC: see paragraph 6.08I(2)(c).

Replaced Authorised Version registered 19/04/2024 F2021C00921

6.08F MSICs—application to Secretary if person has adverse criminal record

(1) If:

(a) a person is not eligible to be issued an MSIC only because he or she:

(i) has an adverse criminal record; or

(ii) has an adverse criminal record, and does not have an operational need for an MSIC; and

(b) he or she has not been convicted of a tier 1 offence;

an issuing body or the applicant may apply to the Secretary, in writing, for approval to issue an MSIC to the person.

Note: If the person does not have an operational need for an MSIC, an MSIC must not be issued to the person until he or she has an operational need (see subregulation (9)).

(2) If the Secretary needs more information to deal with an application, the Secretary may ask the issuing body or applicant, in writing, to provide the information.

(3) Within 30 days after receiving an application (or, if the Secretary has asked for information under subregulation (2), after receiving the information), the Secretary must:

(a) approve, or refuse to approve, in writing, the issuing of the MSIC; and

(b) notify the body, or applicant, in writing of the decision and, if the decision is a refusal, notify the applicant of the reasons for the decision.

Note: Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the decision reviewed.

(4) If the Secretary has not approved, or refused to approve, the issue of the MSIC within the period allowed by subregulation (3), the Secretary is taken to have refused to approve the issue of the MSIC.

(5) Before approving or refusing to approve the issue of the MSIC to a person who is not eligible to be issued an MSIC only because the person's criminal record prevents him or her being issued with an MSIC, the Secretary must decide whether the person constitutes a threat to the security of maritime transport or an offshore facility by considering:

(a) the nature of the offence the person was convicted of; and

(ab) if the person was convicted of the offence before becoming the holder of an MSIC; and

(b) the length of the term of imprisonment imposed on him or her; and

(c) if he or she has served the term, or part of the term—how long it is, and his or her conduct and employment history, since he or she did so; and

(d) if the whole of the sentence was suspended—how long the sentence is, and his or her conduct and employment history, since the sentence was imposed; and

(e) anything else relevant that the Secretary knows about.

(6) The Secretary may give an approval subject to a condition, but must notify the issuing body in writing what the condition is.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(7) Subregulation (8) applies if the Secretary, under paragraph (3)(b), notifies the body or applicant that he or she has refused to approve the issuing of an MSIC.

(8) If the Secretary thinks it is necessary to do so to prevent unlawful interference with maritime transport or offshore facilities, or to prevent the use of maritime transport or offshore facilities in connection with serious crime, he or she may:

(a) direct the issuing body to which the person applied for the issue of an MSIC, in writing, to give the Secretary the following information:

(i) the name of the person's employer;

(ii) the kind of business that the employer is engaged in; and

(b) give a written notice to the person's employer, a maritime industry participant or both:

(i) stating that, following a background check, the Secretary has refused to approve the issue of an MSIC to the person; and

(ii) stating the information provided by the issuing body following a direction under paragraph (a).

Applicant who does not have an operational need

(9) If the Secretary approves the issue of an MSIC to a person who does not have an operational need for the MSIC, the MSIC must not be issued until the person has an operational need for the MSIC.

6.08H Persons the subject of qualified security assessments

(1) If a security assessment of a person who applied to an issuing body for the issue of an MSIC is a qualified security assessment, the Secretary must:

(a) if the Secretary is satisfied that the holding of an MSIC by the person would not constitute a threat to the security of maritime transport or an offshore facility—give the issuing body a written notice stating that an MSIC may be issued because the person is not a threat to the security of maritime transport or an offshore facility; or

(b) if the Secretary is satisfied that the holding of an MSIC by the person would constitute a threat to the security of maritime transport or an offshore facility—give the issuing body a written direction not to issue the MSIC to the person.

Note: For a person's notification and review rights in relation to a qualified security assessment, see section 38 and Division 4 of Part IV of the *Australian Security Intelligence Organisation Act 1979.*

(2) The Secretary must give the person a notice stating that the Secretary has given the issuing body a notice under paragraph (1)(a) or a direction under paragraph (1)(b).

(3) An issuing body must not issue an MSIC to a person in contravention of a direction under paragraph (1)(b).

Penalty: 20 penalty units.

Replaced Authorised Version registered 19/04/2024 F2021C00921

6.08HA Provision of information to Secretary AGD

If the Secretary makes a decision under regulation 6.08F, 6.08H, 6.08MB, 6.08MC or 6.08X, the Secretary must tell the Secretary AGD about the decision.

6.08I MSICs—period of issue and expiry

(1) Unless earlier cancelled, an MSIC expires:

(a) if the holder applied for a white MSIC, or a blue MSIC that is to be in force for 2 years—2 years after the last day of the month in which the background check, undertaken when the holder applied for the MSIC, was completed; or

(b) if the holder applied for a blue MSIC that is to be in force for 4 years—4 years after the last day of the month in which the background check, undertaken when the holder applied for the MSIC, was completed.

(2) However:

(a) an MSIC issued to a person under 18 in reliance on subregulation 6.08C(4) must expire no later than the earlier of:

(i) 6 months after the person's 18th birthday; and

(ii) 2 years after the last day of the month in which the background check, undertaken when the person applied for the MSIC, was completed; and

(b) an MSIC issued to a person who is entitled to remain in Australia because he or she holds a visa must expire no later than the day on which the person's visa expires; and

(c) an MSIC issued under regulation 6.08E must expire on the same day as the ASIC mentioned in paragraph 6.08E(a); and

(d) an MSIC issued to a person on the basis of being a person mentioned in subparagraph 6.08C(1)(c)(iii) must expire no later than 2 years after the last day of the month in which the background check, undertaken when the person applied for the MSIC, was completed; and

(e) an MSIC issued under regulation 6.08L expires in accordance with subregulation 6.08L(3).

(3) If an MSIC is suspended under regulation 6.08LF, the MSIC expires on the date it would have expired if it had not been suspended.

(4) If an MSIC is cancelled and the cancellation is set aside (however described) by the Secretary or the Administrative Appeals Tribunal, the MSIC expires on the earlier of:

(a) the date it would have expired if it had not been cancelled; or

(b) if a condition imposed under subregulation 6.08MD(1) sets an earlier expiry date—that date.

Replaced Authorised Version registered 19/04/2024 F2021C00921

6.08J Form of blue MSICs and white MSICs

Form of blue MSIC

(2) A blue MSIC issued by an issuing body must be in a form approved in writing by the Secretary for the issuing body.

Form of white MSIC

(3) A white MSIC issued by an issuing body must be in a form approved in writing by the Secretary for the issuing body.

General

(4) Without limiting subregulation (2) or (3), the approval of a form under subregulation (2) or (3) may extend to specifying any or all of the following:
  (a) the dimensions of an MSIC and each of its parts;
  (b) the information that must be included on the front or the back of an MSIC;
  (c) the security features that must be incorporated into an MSIC;
  (d) the kind of photograph of the holder of an MSIC that must be included on the MSIC, including the size and quality of the photograph.

(4A) The Secretary may approve a form of an MSIC for an issuing body under this regulation only if the Secretary is reasonably satisfied that it is necessary to do so for the purposes of safeguarding against unlawful interference with maritime transport or offshore facilities.

(5) The Secretary may approve the issue of an MSIC showing the holder's name on the back if the Secretary is satisfied that having the holder's name on the front would put the holder's personal security at risk.

(6) A person commits an offence if:
  (a) the person is an issuing body; and
  (b) the Secretary gives the person a copy of a form approved for the issuing body under this regulation for a blue MSIC or a white MSIC; and
  (c) the person issues a blue MSIC or a white MSIC; and
  (d) the MSIC issued does not comply in a particular respect with the form approved for the issuing body for that kind of MSIC; and
  (e) the respect in which the form does not comply is not the subject of an approval under subregulation (5).

Penalty: 50 penalty units.

(7) An offence under subregulation (6) is an offence of strict liability.

Note 1: For ***strict liability***, see section 6.1 of the *Criminal Code*.

Note 2: National Privacy Principle 7, set out in Schedule 3 to the *Privacy Act 1988*, restricts the uses to which an identifier of an individual can be put.

Replaced Authorised Version registered 19/04/2024 F2021C00921

6.08JA Issuing body to be given copy of approved form of MSIC

(1) The Secretary must, as soon as practicable after approving a form of an MSIC for an issuing body under regulation 6.08J, give a copy of the approved form to the issuing body.

(2) The Secretary may, in the copy of the approved form given to the issuing body, direct that the issuing body must not disclose the details of the approved form to another person except in the circumstances specified in the direction.

(3) A person commits an offence if:
  (a) the person is an issuing body; and
  (b) the Secretary, under subregulation (1), gives the issuing body a copy of a form approved for the issuing body; and
  (c) the copy of the approved form contains a direction under subregulation (2); and
  (d) the issuing body contravenes the direction.

  Penalty: 50 penalty units.

(4) An offence under subregulation (3) is an offence of strict liability.

  Note: For strict liability, see section 6.1 of the *Criminal Code*.

6.08JB Issuing body may disclose details of approved form to other persons

(1) An issuing body may, in the circumstances specified in a direction in a copy of an approved form given to the issuing body under regulation 6.08JA, disclose the details of the approved form to another person.

(2) A person commits an offence if:
  (a) an issuing body discloses the details of an approved form to the person in in accordance with subregulation (1); and
  (b) the person discloses the details to another person without the written approval of the Secretary.

  Penalty: 50 penalty units.

(3) An offence under subregulation (2) is an offence of strict liability.

  Note: For strict liability, see section 6.1 of the *Criminal Code*.

6.08K Temporary MSICs

(1) A temporary MSIC may be issued to a person by a maritime industry participant if:
  (a) either:
    (i) the person is the holder of a blue MSIC and has forgotten the MSIC, or it has been lost, stolen or destroyed; or
    (iii) subregulation (2A) applies to the person; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(b) the participant is shown a document that provides evidence of the identity of the person; and

(c) the participant's maritime security plan, ship security plan or offshore security plan provides for the participant to:

(i) issue temporary MSICs; and

(ii) create, and keep for auditing purposes, a register of those temporary MSICs; and

(d) the participant acts in accordance with its security plan.

(2A) This subregulation applies to a person if:

(a) the person's application for the issue of a blue MSIC has been approved by the issuing body; and

(b) he or she has not yet received the MSIC.

(3) A temporary MSIC expires on the day specified by the participant.

(6) If the participant issues a temporary MSIC to a person to whom subregulation (2A) applies, the temporary MSIC will expire on the earliest of the following:

(a) the beginning of the day 2 months after the day when the temporary MSIC is issued;

(b) the day the MSIC holder receives his or her blue MSIC.

6.08KA Form of temporary MSICs

(1) Subject to subregulation (3), a temporary MSIC must comply with the following requirements:

(a) it must be orange in colour and no smaller than 54 mm wide by 86 mm high;

(b) it must have a black capital letter 'T' in Arial of at least 125 point on the front;

(c) it must display, or include, the following information:

(i) the holder's name as it appears on the holder's blue MSIC;

(ii) the unique identifying number that appears on the holder's blue MSIC;

(iii) a description of the document that provided evidence of the identity of the holder;

(iv) the name of the maritime industry participant that issued the temporary MSIC;

(v) a description of the maritime security zone or zones in which the blue MSIC is valid;

(vi) the expiry date of the temporary MSIC.

(2) For paragraph (1)(c), information may be included on a temporary MSIC by:

(a) writing it by hand; or

(b) using a printing process; or

(c) encoding it magnetically, or in another way.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(3) The Secretary may approve, in writing, the issue of a temporary MSIC that does not comply with subregulation (1) or (2).

6.08L Issue of replacement MSICs

(1) An issuing body may issue a replacement MSIC (the ***replacement MSIC***) to the holder of another MSIC (the ***old MSIC***) issued by the issuing body if:

(a) any of the following apply:

(i) the old MSIC has been lost or destroyed, and the holder has given the issuing body a statutory declaration setting out the circumstances of the loss or destruction (which may be in the same document as the declaration referred to in paragraph (d));

(ii) the old MSIC has been stolen, and the holder has given the issuing body a copy of a police report, or other information issued by the police, regarding the theft;

(iii) the holder's name has changed, and the holder has notified the issuing body of the change in accordance with regulation 6.08LCA;

(iv) the holder wishes to replace the old MSIC with the replacement MSIC because the holder has an operational need for the replacement MSIC; and

(b) the holder has an operational need for the replacement MSIC; and

(c) in a case where the replacement MSIC is a different kind of MSIC from the old MSIC—the holder has given the issuing body evidence of the holder's operational need for the replacement MSIC; and

(d) the holder has given the issuing body a statutory declaration stating that, since his or her background checks were completed, he or she has not been convicted of a maritime-security-relevant offence.

Issue of replacement MSIC

(2) The replacement MSIC may be a blue MSIC or a white MSIC.

Note: The holder must have an operational need for the replacement MSIC (see paragraph (1)(b)).

(3) The replacement MSIC expires:

(a) if the replacement MSIC is a blue MSIC—at the same time as the old MSIC would have expired; and

(b) if the replacement MSIC is a white MSIC—at the earlier of the following times:

(i) the same time as the old MSIC would have expired;

(ii) 2 years after the last day of the month in which the background check, undertaken when the holder applied for the old MSIC, was completed.

(4) The replacement MSIC is subject to:

(a) any conditions to which the old MSIC was subject; and

(b) any conditions which the issuing body imposes on the replacement MSIC by written notice given to the holder of the replacement MSIC.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(5) The number of the replacement MSIC must be unique among MSICs issued by the issuing body.

(6) Either:
  (a) the replacement MSIC must bear a number indicating how many times a permanent MSIC has been issued to the person with the same expiry date; or
  (b) the issuing body must keep a record of how many times it has issued a permanent MSIC to the person with that expiry date.

(7) The issue of a replacement MSIC to a person under this regulation cancels any temporary MSIC the person holds under regulation 6.08K.

6.08LA Special arrangements for persons with visa extensions

An issuing body may issue an MSIC to a person, if the person:
  (a) was the holder of an MSIC (the ***old MSIC***) that expired because the person's visa (the ***old visa***) has expired; and
  (b) holds a new visa entitling him or her to work in Australia, that was issued less than 12 months after the expiry of the old visa; and
  (c) has an operational need to hold the MSIC that the issuing body proposes to issue; and
  (d) gives the issuing body a statutory declaration stating that, since the expiry of the old visa, none of the information given in relation to the application for the old MSIC has changed.

6.08LB Obligation of applicants for, and holders of, MSICs—conviction of maritime-security-relevant offence

(1) Subregulation (2) applies if a person who is an applicant for, or the holder of, an MSIC is:
  (a) convicted of and sentenced for a tier 1 offence or tier 2 offence; or
  (b) convicted of, and sentenced to imprisonment for, a tier 3 offence.

(2) Within 7 days after being sentenced, the person must notify the issuing body or the Secretary in writing of the following matters:
  (a) his or her name, date of birth and residential address;
  (b) if he or she holds one or more MSICs—the unique number of each MSIC held;
  (c) the date he or she was convicted and sentenced;
  (d) the court in which he or she was convicted;
  (e) whether he or she gives consent for:
    (i) his or her identity to be confirmed; and
    (ii) new background checks to be undertaken; and
    (iii) the outcome of the background checks to be provided to the issuing body, if the outcome will adversely affect his or her ability to hold an MSIC or to continue holding the MSIC.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Penalty: 20 penalty units.

Note: For the meaning of ***maritime-security-relevant offence***, see regulation 6.07B.

(3) The issuing body or the Secretary may, if not satisfied that all of the information mentioned in subregulation (2) has been provided, request that the person provide that information within 14 days.

(4) For paragraph (2)(e), consent is given if the person gives consent and any information requested to confirm his or her identity to:
  (a) if the person notified the issuing body under subregulation (1)—the issuing body; or
  (b) if the person notified the Secretary under subregulation (1)—the Secretary.

(5) The Secretary must tell the issuing body if the person:
  (a) notifies the Secretary under subregulation (2); and
  (b) does not:
    (i) give his or her consent under paragraph (2)(e); or
    (ii) comply with:
      (A) all of the requirements of subregulation (2); and
      (B) any request under subregulation (3) within 14 days after the request.

6.08LBA Obligation on issuing body notified under regulation 6.08LB

An issuing body for an MSIC commits an offence if:
  (a) a person who is an applicant for, or the holder of, an MSIC notifies the issuing body of the matters mentioned in subregulation 6.08LB(2); and
  (b) the issuing body fails to apply to the Secretary AGD for a background check on the person within 2 working days after the person:
    (i) notifies of his or her consent under paragraph 6.08LB(2)(e); or
    (ii) if any information is requested under subregulation 6.08LB(3)—provides that information.

Penalty: 100 penalty units.

6.08LC Application by Secretary for background check on applicant for, or holder of, MSIC

(1) The Secretary may apply to the Secretary AGD for a background check on a person who is an applicant for, or the holder of, an MSIC if the Secretary considers on reasonable grounds that the person:
  (a) has been convicted of a maritime-security-relevant offence; or
  (b) constitutes a threat to maritime transport or offshore facility security.

(2) In considering the matter mentioned in paragraph (1)(a) or (b), the Secretary must take into account:
  (a) any information provided to the Secretary by the person or the issuing body for the MSIC; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(b) any information provided to the Secretary by the Secretary AGD or a law enforcement agency (however described) about the person; and
(c) anything else relevant that the Secretary knows about.

6.08LCA Obligation of applicants for, and holders of, MSICs—change of name

(1) A person commits an offence of strict liability if:
(a) the person is an applicant for, or a holder of, an MSIC; and
(b) the person changes his or her name; and
(c) the person does not notify the issuing body to which the application was made or which issued the MSIC (as the case requires) of the change, in accordance with subregulation (2), within 30 days after the change.

Penalty: 5 penalty units.

(2) The person must:
(a) notify the issuing body in person; and
(b) at the same time, give the issuing body an original of a current and valid document, showing the new name, which was issued to the person by a Commonwealth, State or Territory Department or agency.

(3) The issuing body must notify AusCheck of the change of name, using the AusCheck facility, within 7 days.

Note: For the issuing of a replacement MSIC to an MSIC holder who changes his or her name, see regulation 6.08L.

6.08LD Obligation of MSIC holders issued with cards for more than 2 years—change of address

(1) A holder of an MSIC commits an offence if:
(a) the holder's MSIC was issued for more than 2 years; and
(b) the holder's residential address has changed since the holder applied for the MSIC; and
(c) the holder fails to notify, in writing, the issuing body that issued the MSIC of all the changes to the holder's residential address since the holder applied for the MSIC; and
(d) the notification is not made by the time mentioned in subregulation (3).

Penalty: 5 penalty units.

(3) For paragraph (1)(d), the time is no later than 2 years and 30 days before the day of expiry mentioned on the front of the holder's MSIC.

6.08LDA Obligation of issuing bodies—notification of change of address

An issuing body for an MSIC commits an offence if:
(a) the holder of an MSIC notifies the issuing body of the change of his or her residential address in accordance with regulation 6.08LD; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(b) the issuing body fails, within 7 days of being notified of the change, to update the AusCheck facility with the changed address.

Penalty: 50 penalty units.

6.08LE Suspension of MSICs—Secretary's direction

(1) The Secretary may, in writing, direct an issuing body to suspend an MSIC if:
   (a) the holder of the MSIC has been convicted of a maritime-security-relevant offence, but has not yet been sentenced for the offence; and
   (b) the Secretary reasonably considers that either:
      (i) the holder of the MSIC constitutes a threat to the security of maritime transport or an offshore facility; or
      (ii) there is a risk that the holder of the MSIC may use maritime transport or an offshore facility in connection with serious crime.

(2) In considering whether subparagraph (1)(b)(i) or (ii) applies, the Secretary must consider:
   (a) the type of offence the holder was convicted of and the circumstances in which the offence was committed; and
   (b) the effect the suspension may have on the holder's employment; and
   (c) if the holder is employed in a maritime security zone—the location of the maritime security zone; and
   (d) whether the holder is employed in a port security zone, ship security zone, on-board security zone or offshore security zone, and the type of area in which the holder is employed; and
   (e) anything else relevant that the Secretary knows about.

(3) If the Secretary makes a direction under subregulation (1), the Secretary must tell the Secretary AGD, in writing, about the direction.

6.08LF Suspension of MSICs by issuing body

(1) An issuing body must immediately suspend an MSIC issued by the body if directed to do so by the Secretary.

(2) As soon as practicable after the issuing body suspends the MSIC, the body must tell the holder of the MSIC, in writing, that the MSIC has been suspended and the reasons for the suspension.

Note: Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice, in writing, of the making of the decision and of the person's right to have the decision reviewed.

(3) The suspension takes effect when the holder is told about the suspension.

(4) The holder of a blue MSIC that is suspended under this regulation must return the MSIC to the issuing body for the MSIC not later than 7 days after the day the holder is told in writing that the MSIC has been suspended.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Penalty: 10 penalty units.

(5) An offence against subregulation (4) is an offence of strict liability.

6.08LG Period of suspension of MSIC

(1) Unless subregulation (2) applies, the suspension of an MSIC continues until the MSIC is cancelled or expires.

(2) If:

(a) the Secretary notifies the issuing body that issued the MSIC of the outcome of a background check of the holder of the MSIC; and

(b) the issuing body is not required under regulation 6.08M to cancel the MSIC;

the suspension of the MSIC ends on the day after the issuing body is notified.

Note: Provisions relating to the conduct of a background check when the holder of an MSIC has been convicted of a maritime-security-relevant offence include regulations 6.08BA and 6.08LB of these Regulations, and section 8 of the *AusCheck Regulations 2017*.

6.08LH Suspension of temporary MSIC

(1) This regulation applies if a person holds:

(a) an MSIC that is suspended; and

(b) a temporary MSIC.

(2) The temporary MSIC is suspended:

(a) when the MSIC is suspended; and

(b) for the period the MSIC is suspended.

6.08LI Report to Secretary of suspension of MSIC

(1) If an issuing body suspends an MSIC, the body must, not later than 7 days after the day the MSIC is suspended, tell the Secretary, in writing:

(a) about the suspension; and

(b) the name, date of birth and residential address of the holder of the MSIC.

Note: An issuing body may suspend an MSIC only when directed by the Secretary—see subregulation 6.08LF(1).

(2) The Secretary may tell the holder's employer, or a maritime industry participant, that the MSIC has been suspended if the Secretary considers on reasonable grounds that doing so may help to prevent unlawful interference with maritime transport or offshore facilities.

6.08M Cancellation of MSICs

(1) An issuing body must immediately cancel an MSIC issued by the body if:

(a) the body finds out that the MSIC was not issued in accordance with the body's MSIC plan; or

Replaced Authorised Version registered 19/04/2024 F2021C00921

(b) the Secretary finds out that the MSIC was not issued in accordance with the body's MSIC plan and notifies the issuing body in writing; or

(c) the Secretary has notified the issuing body in writing that a security assessment of the holder was adverse; or

(ca) the Secretary has told the issuing body in writing that the holder has received a qualified security assessment; or

(d) the body finds out that the holder is not entitled to work in Australia, and the holder is not a person mentioned in subparagraph 6.08C(1)(c)(iii); or

(e) subject to subregulation (1A), the issuing body has received a notice from the Secretary that the holder has an adverse criminal record; or

(ea) the Secretary advises the issuing body that a background check of the holder has been cancelled under section 11A of the *AusCheck Regulations 2017*; or

(eb) the holder of an MSIC that is issued for more than 2 years withdraws consent for a background check before an application for the check is taken to be made under subsection 10(2) of the *AusCheck Regulations 2017*; or

(ec) both of the following apply:

(i) an application for a background check of the holder is made under regulation 6.08BA or 6.08LC of these Regulations or subsection 9(2), 10(2) or 16A(3) of the *AusCheck Regulations 2017*;

(ii) the Secretary AGD advises the issuing body under section 15A of the *AusCheck Regulations 2017* that the background check is cancelled; or

(f) the holder no longer has an operational need to hold the MSIC; or

(g) the body finds out that, for a continuous period of 12 months, the holder has not had an operational need to hold the MSIC; or

(h) the holder:

(i) notifies the Secretary or the issuing body under regulation 6.08LB that the holder has been convicted of and sentenced for a maritime-security-relevant offence; and

(ii) does not consent to a background check or does not comply with subregulation 6.08LB(2) and, if requested, subregulation 6.08LB(3); or

(i) the issuing body finds out that the MSIC has been lost, stolen or destroyed; or

(j) the issuing body issues a replacement MSIC under regulation 6.08L for a reason referred to in subparagraph 6.08L(1)(a)(iii) (change of name) or 6.08L(1)(a)(iv) (operational need for replacement MSIC); or

(k) the issuing body finds out that the holder has changed his or her name, and the holder has not asked the issuing body to issue a replacement MSIC under regulation 6.08L.

(1A) An issuing body must not cancel an MSIC that was:

(a) issued with the approval of the Secretary under regulation 6.08F; or

(b) reinstated under regulation 6.08MC;

if:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(c) the notice that the holder has an adverse criminal record relates to an application for a new MSIC; or

(d) the Secretary advises the issuing body that there has been no material change in the holder's criminal history.

(2) As soon as practicable after an issuing body cancels an MSIC under subregulation (1), the body must notify the holder, in writing, that the MSIC has been cancelled and the reasons for the cancellation.

Note: Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person's right to have the decision reviewed.

(2A) An issuing body commits an offence if:

(a) the issuing body is required to cancel an MSIC under paragraph (1)(c), (ca), (e), (ea) or (eb); and

(b) the issuing body fails to immediately cancel the MSIC.

Penalty: 50 penalty units.

(2B) An issuing body commits an offence if:

(a) the issuing body cancels an MSIC under paragraph (1)(c), (ca), (e), (ea) or (eb); and

(b) the issuing body fails to tell the holder of the MSIC, in writing, as soon as practicable after the day the MSIC is cancelled, that the MSIC has been cancelled and the reasons for the cancellation.

Penalty: 50 penalty units.

(3) A cancellation under subregulation (1) takes effect when the holder is notified of it in writing.

(4) Any temporary MSIC issued to the holder is cancelled if the holder's MSIC is cancelled.

(5) The cancellation of the temporary MSIC takes effect at the time the cancellation of the MSIC takes effect.

6.08MA Reinstatement of cancelled MSIC—application

(1) This regulation applies if an MSIC is cancelled by an issuing body under paragraph 6.08M(1)(ca) or (e).

(2) The former holder of the MSIC or the issuing body may apply to the Secretary, in writing, for the cancellation to be set aside.

(3) The application must be made not later than 28 days after the day the former holder of the MSIC is told about the cancellation.

(4) If the Secretary needs more information to deal with an application, the Secretary may ask the former holder of the MSIC or the issuing body, in writing, to provide the information.

Replaced Authorised Version registered 19/04/2024 F2021C00921

6.08MB Reinstatement of MSIC cancelled for qualified security assessment—Secretary's decision

(1) This regulation applies if:
  (a) an MSIC is cancelled under paragraph 6.08M(1)(ca); and
  (b) the Secretary receives:
    (i) an application mentioned in subregulation 6.08MA(2) from the applicant; or
    (ii) if the Secretary asks the former holder of the MSIC or the issuing body for the MSIC for information under subregulation 6.08MA(4)—the information.

(2) If the Secretary is satisfied on reasonable grounds that setting aside the cancellation of the MSIC would not constitute a threat to the security of maritime transport or an offshore facility, the Secretary must set aside the cancellation.

(3) If the Secretary is satisfied on reasonable grounds that setting aside the cancellation of the MSIC would constitute a threat to the security of maritime transport or an offshore facility, the Secretary must refuse to set aside the cancellation.

(4) Within 30 days after the day the Secretary receives the application or, if subparagraph (1)(b)(ii) applies, within 30 days after the day the Secretary receives the information, the Secretary must:
  (a) decide whether to set aside the cancellation of the MSIC; and
  (b) if the Secretary decides to set aside the cancellation—tell the following persons, in writing, about the decision and any conditions under regulation 6.08MD to which the setting aside is subject:
    (i) the applicant;
    (ii) the Secretary AGD;
    (iii) if the applicant is the former holder of the MSIC—the issuing body;
    (iv) if the applicant is the issuing body—the former holder of the MSIC; and
  (c) if the Secretary refuses to set aside the cancellation:
    (i) tell the former holder of the MSIC, in writing, about the decision and the reasons for it; and
    (ii) if the applicant is the issuing body—tell the issuing body, in writing, about the decision.

Note 1: Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice, in writing, of the making of the decision and of the person's right to have the decision reviewed.

Note 2: For a person's notification and review rights in relation to a qualified security assessment, see section 38 and Division 4 of Part IV of the *Australian Security Intelligence Organisation Act 1979.*

Replaced Authorised Version registered 19/04/2024 F2021C00921

(5) If the Secretary does not make a decision mentioned in paragraph (4)(a) within the period mentioned in subregulation (4), the Secretary is taken to have refused to set aside the cancellation of the MSIC.

(6) In this regulation:

applicant, for a cancelled MSIC, means the person who made the application under subregulation 6.08MA(2) for the cancellation to be set aside.

6.08MC Reinstatement of MSIC cancelled for adverse criminal record—Secretary's decision

(1) This regulation applies if:
  (a) an MSIC is cancelled under paragraph 6.08M(1)(e); and
  (b) the Secretary receives:
    (i) an application mentioned in subregulation 6.08MA(2) from the applicant; or
    (ii) if the Secretary asks the former holder of the MSIC or the issuing body for the MSIC for information under subregulation 6.08MA(4)—the information.

(2) Within 30 days after the day the Secretary receives the application or, if subparagraph (1)(b)(ii) applies, within 30 days after the day the Secretary receives the information, the Secretary must:
  (a) decide whether to set aside the cancellation of the MSIC; and
  (b) if the Secretary decides to set aside the cancellation—tell the following persons, in writing, about the decision and any conditions under regulation 6.08MD to which the setting aside is subject:
    (i) the applicant;
    (ii) the Secretary AGD;
    (iii) if the applicant is the former holder of the MSIC—the issuing body;
    (iv) if the applicant is the issuing body—the former holder of the MSIC; and
  (c) if the Secretary refuses to set aside the cancellation:
    (i) tell the former holder of the MSIC, in writing, about the decision and the reasons for it; and
    (ii) if the applicant is the issuing body—tell the issuing body, in writing, about the decision.

Note: Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice, in writing, of the making of the decision and of the person's right to have the decision reviewed.

(3) If the Secretary does not make a decision mentioned in paragraph (2)(a) within the period mentioned in subregulation (2), the Secretary is taken to have refused to set aside the cancellation of the MSIC.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(4) Before making a decision mentioned in paragraph (2)(a), the Secretary must decide whether the former holder constitutes a threat to the security of maritime transport or an offshore facility by considering:

(a) the type and length of the term of imprisonment imposed on the former holder; and

(b) if the former holder has served the term, or part of the term—how long it is, and the former holder's conduct, since the term was served; and

(c) whether the former holder was convicted of the offence before becoming the holder of an MSIC; and

(d) the effect on the holder's employment if the MSIC is cancelled; and

(e) the location of the maritime security zone where the holder is employed; and

(f) whether the holder is employed in a port security zone, ship security zone, on-board security zone or offshore security zone and the type of area in which the holder is employed; and

(g) anything else relevant that the Secretary knows about.

(5) In this regulation:

applicant, for a cancelled MSIC, means the person who made the application under subregulation 6.08MA(2) for the cancellation to be set aside.

6.08MD Reinstatement of MSIC subject to condition

(1) The Secretary may set aside a cancellation mentioned in regulation 6.08MB or 6.08MC subject to a condition.

Example: A condition that background checking is conducted at stated intervals.

(2) If the former holder of the MSIC applied for the cancellation to be set aside, and the Secretary sets the cancellation aside subject to a condition, the Secretary must tell the issuing body for the MSIC, in writing, about the condition.

(3) If the issuing body for the MSIC applied for the cancellation to be set aside, and the Secretary sets the cancellation aside subject to a condition, the Secretary must tell the former holder of the MSIC, in writing, about the condition.

6.08N Cancellation of MSICs at holder's request

(1) An issuing body must cancel an MSIC issued by the body if the holder of the MSIC asks the body to cancel it.

(2) The cancellation of a blue MSIC under subregulation (1) takes effect when the MSIC is returned to the issuing body.

(3) The cancellation of a white MSIC under subregulation (1) takes effect when the issuing body receives the request.

Replaced Authorised Version registered 19/04/2024 F2021C00921

6.08O Report to Secretary of cancellation of MSIC

(1) If an issuing body cancels an MSIC, the body must, within 7 days after the cancellation, notify the Secretary in writing:
  (a) the holder's name, address and date of birth; and
  (b) the reason for the cancellation.

(2) If the cancellation is for a reason mentioned in a paragraph of subregulation 6.08M(1), the Secretary may notify the employer of the former holder of the MSIC, or a maritime industry participant, that the MSIC has been cancelled.

(3) The Secretary may act under subregulation (2) only if he or she thinks that doing so may help to prevent unlawful interference with maritime transport or offshore facilities, or the use of maritime transport or offshore facilities in connection with serious crime.

6.08P Return of blue MSICs that have expired etc.

(1) The holder of a blue MSIC must return it to an issuing body 30 days or less after:
  (a) the MSIC expires; or
  (b) the holder is notified that it has been cancelled; or
  (c) the MSIC has been damaged, altered or defaced (permanently or temporarily).

  Penalty: 10 penalty units.

(2) A contravention of subregulation (1) is an offence of strict liability.

6.08Q Holder no longer needing blue MSIC

(1) The holder of a blue MSIC is guilty of an offence if:
  (a) he or she becomes aware of circumstances that will result in him or her not having an operational need to hold the MSIC for 12 months; and
  (b) he or she fails to return it to an issuing body within 30 days of becoming aware of the circumstances.

  Penalty: 5 penalty units.

(2) Strict liability applies to paragraph (1)(b).

6.08R Notification of lost, stolen and destroyed blue MSICs

(1) The holder of a blue MSIC commits an offence if:
  (a) the MSIC has been lost, stolen or destroyed; and
  (b) the holder of the MSIC knows about the loss, theft or destruction; and
  (c) he or she does not:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(i) make a report, in the form of a statutory declaration, of the loss to the issuing body that issued the MSIC within 7 days of becoming aware of the loss, theft or destruction; or

(ii) if the MSIC was stolen—give the issuing body a copy of a police report, or other information issued by the police, regarding the theft, within 7 days of becoming aware of the theft.

Penalty: 10 penalty units.

(2) Strict liability applies to paragraph (1)(c).

(3) However, subregulation (1) does not apply if the MSIC has been destroyed by the issuing body that issued it.

Subdivision 6.1A.5—Powers of security officers in relation to MSICs and temporary MSICs

6.08S Directions to show valid MSICs, temporary MSICs or other identification

(1) In this regulation:

security officer means:

(a) a law enforcement officer; or

(b) a maritime security inspector.

(2) If a person is in a part of a maritime security zone and apparently not properly displaying a valid MSIC or valid temporary MSIC, a security officer may (unless he or she knows the person to be an exempt person in relation to that part of the zone) direct the person to show him or her:

(a) a valid blue MSIC or valid temporary MSIC; or

(b) identification that establishes that the person is an exempt person.

(3) Before directing the person to do so, the security officer must show the person:

(a) the officer's identity card; or

(b) another appropriate form of identification.

(4) A person must comply with a direction of a security officer under subregulation (2).

Penalty: 10 penalty units.

Subdivision 6.1A.6—Record-keeping

6.08T Register of MSICs

(1) An issuing body must keep a register in accordance with this regulation.

(2) The register must contain the following details of each MSIC issued by the body to a person:

(a) his or her name and telephone number (if any);

Replaced Authorised Version registered 19/04/2024 F2021C00921

(b) a copy of the photograph that appears on his or her MSIC;
(c) subject to subregulation (3), his or her residential address;
(d) the general reason that he or she has an operational need to hold an MSIC;
(e) the documents used to decide about his or her eligibility for an MSIC;
(f) the date of the beginning of the current period during which he or she has continuously held an MSIC;
(g) the unique number of the MSIC;
(h) its date of issue;
(i) its date of expiry;
(j) if applicable, the date on which it was cancelled;
(ja) if the MSIC is cancelled and the cancellation is set aside by the Secretary or set aside (however described) by the Administrative Appeals Tribunal:
(i) the date the cancellation is set aside; and
(ii) if the holder returns the MSIC to the issuing body following the cancellation—the date the body returns the MSIC to the holder;
(jb) if the MSIC is suspended:
(i) the date the issuing body tells the holder about the suspension; and
(ii) if the holder returns the MSIC to the issuing body following the suspension—the date the body returns the MSIC to the holder; and
(iii) if the suspension period ends under subregulation 6.08LG(2)—the date the body returns the MSIC to the holder.
(k) if applicable, the date or dates on which it was reported lost, stolen or destroyed.

(3) The register need not contain the residential address of an MSIC holder who is:
(a) a law enforcement officer; or
(b) an officer or employee of ASIO; or
(c) an employee of a Commonwealth authority.

6.08U Other records of issuing bodies

(1) An issuing body must maintain records that are sufficient to demonstrate that it has complied with its MSIC plan.

(2) The issuing body must retain the following, in relation to an application for the issuing body to issue an MSIC to a person:
(a) a copy of the application;
(b) if the issuing body issues the MSIC to the person—the record of issue of the MSIC;
(c) copies of the identification documents that were given to the issuing body in relation to the application;
(d) any records, or copies of any documents, that were given to the issuing body in relation to the applicant's operational need for the MSIC.

(2A) The records and documents required to be retained under subregulation (2) must be retained until:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(a) if the issuing body issues the MSIC to the person—the end of 3 years after the completion of the background check most recently requested in relation to the application or the MSIC; or

(b) otherwise—the end of 3 years after the application was made.

(3) The records and documents may be kept by means of a computer or in any other form that can be conveniently audited.

(5) The issuing body must allow a maritime security inspector to inspect the records and documents on request, subject to reasonable notice.

6.08V Annual reporting

An issuing body must report to the Secretary in writing, within 1 month after the end of each financial year:

(a) the total number of MSICs issued by the body; and

(b) the number of MSICs issued by the body that have not expired and have not been cancelled; and

(c) the number of blue MSICs issued by the body that have expired or been suspended or cancelled, but have not been returned to the body; and

(d) the number of MSICs issued by the body that were cancelled in the financial year to which the report relates; and

(e) the number of MSICs issued by the body that expired in that financial year; and

(f) the number of MSICs issued by the body that were suspended in the financial year to which the report relates.

Penalty: 20 penalty units.

Subdivision 6.1A.7—Review of decisions

6.08W Definitions

In this Subdivision:

AAT Act means the *Administrative Appeals Tribunal Act 1975*.

decision has the same meaning as in the AAT Act.

Tribunal means the Administrative Appeals Tribunal.

6.08X Reconsideration of decisions in relation to MSICs and related matters

Decisions in relation to issuing bodies

(1) Application may be made to the Secretary for reconsideration of a decision of the Secretary:

(a) to refuse to authorise a person as an issuing body; or

(b) to impose a condition on an issuing body; or

Replaced Authorised Version registered 19/04/2024 F2021C00921

(c) to direct an issuing body to vary its MSIC plan; or
(d) to refuse to approve a variation of an issuing body's MSIC plan; or
(e) to refuse to exempt an issuing body from giving effect to its MSIC plan in a particular case or respect; or
(f) to impose a condition on an exemption; or
(g) to revoke an issuing body's authorisation; or
(h) to refuse to revoke an issuing body's authorisation.

Decisions in relation to issue, suspension and cancellation of MSICs

(3) Application may be made to the Secretary for:
(a) reconsideration of a decision of the Secretary to:
(i) refuse to approve the issue of an MSIC; or
(ii) impose a condition on an MSIC; or
(iii) direct the suspension of an MSIC; or
(iv) give the issuing body for an MSIC a direction under paragraph 6.08H(1)(b); or
(v) refuse to set aside the cancellation of an MSIC under regulation 6.08MB or 6.08MC; or
(vi) set aside the cancellation of an MSIC subject to a condition under regulation 6.08MD; or
(b) review of a decision of an issuing body to:
(i) refuse to issue an MSIC to somebody; or
(ii) issue an MSIC subject to a condition; or
(iii) cancel an MSIC; or
(iv) suspend an MSIC.

Decisions relating to alternative identification requirements

(3A) Applications may be made to the Tribunal for review of decisions of the Secretary under paragraph 6.08BC(5)(a) to refuse to approve alternative identification requirements for a person.

Decisions in relation to wearing and use of MSICs

(4) Application may be made to the Secretary for reconsideration of a decision of the Secretary:
(a) to refuse to exempt somebody from displaying a valid MSIC in a maritime security zone, or part of such an area; or
(b) to impose a condition on such an exemption.

Decisions in relation to the substituted exercise of the powers of an issuing body

(5) Application may be made to the Secretary for reconsideration of a decision of the Secretary:
(a) to authorise, or refuse to authorise, a person to perform the functions, or exercise the powers, of an issuing body; or

Replaced Authorised Version registered 19/04/2024 F2021C00921

(b) to authorise a person to perform the functions or exercise the powers of an issuing body subject to a condition.

Decisions in relation to issue of disqualifying notice

(6) Application may be made to the Secretary for reconsideration of a decision of the Secretary to issue a disqualifying notice under regulation 6.08D.

6.08Y If Secretary makes no decision

If a person applies to the Secretary under regulation 6.08X for reconsideration or review of a decision and, 30 days after making the application, the Secretary has not notified his or her decision about the application to the applicant, the Secretary is taken to have refused to vary the original decision.

6.08Z AAT review of Secretary's decisions

Application may be made under the AAT Act to the Tribunal for review of a decision made by the Secretary as a result of an application under regulation 6.08X.

Subdivision 6.1A.8—Miscellaneous

6.09A Recovery of costs and expenses (Act ss 105, 109, 113 and 113D)

For subsections 105(4), 109(4), 113(4) and 113D(4) of the Act:

(a) an issuing body may recover costs and expenses reasonably incurred by the body in relation to the issue of an MSIC from the person who asks the body to issue the MSIC; and

(b) a maritime industry participant may recover costs and expenses reasonably incurred by the participant in relation to the issue of a temporary MSIC from the person who asks the participant to issue the temporary MSIC.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 6.2—Port security zones

Subdivision 6.2.1—General

6.20 Types of port security zones

For subsection 103(1) of the Act, the following are prescribed as the types of port security zones that the Secretary may establish within a security regulated port:

(a) land-side restricted zones;

(b) cleared zones;

(c) water-side restricted zones.

6.25 Security barriers

(1) A fence, free standing wall, building or other similar object, or a series of objects such as trees, booms, marker buoys and other similar objects, may constitute a ***security barrier*** if the object or series of objects:

(a) clearly defines the boundary of a maritime security zone; and

(b) deters unauthorised access into the zone.

(2) A security barrier for a land-side restricted zone or a cleared zone must:

(a) deter and deny unauthorised access to the zone; and

(b) allow detection of unauthorised access to the zone; and

(c) have access control points to permit authorised access, being access control points that do not present less of a barrier to unauthorised access than the surrounding parts of the security barrier; and

(d) be subject to regular patrols, surveillance or other measures that allow inspection of the security barrier for damage, and that detect and deter unauthorised access.

Subdivision 6.2.2—Land-side restricted zones

6.30 Identification of zones

(1) The boundaries of a land-side restricted zone must be clearly identifiable and defined by means of a security barrier.

(2) Persons who are in or in the vicinity of the security regulated port in which a land-side restricted zone is established must be informed that:

(a) access to the zone is controlled; and

(b) any unauthorised entry into the zone is an offence under these Regulations.

6.33 Duties of port operator

(1) A port operator must monitor and control access to any land-side restricted zone in the security regulated port in which the zone is established.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Penalty: 200 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

6.35 Duties of port facility operator

(1) A port facility operator must monitor and control access to any land-side restricted zone within the boundaries of the port facility.

Penalty: 200 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

6.45 Offences—unauthorised entry

(1) A person must not enter or remain in a land-side restricted zone unless authorised to do so by:

(a) the port operator for the security regulated port; or

(b) the port facility operator for the port facility;

in which the zone is established.

Penalty: 50 penalty units.

(2) A person must not take a vehicle or thing into, or leave a vehicle or thing in, a land-side restricted zone unless authorised to do so by:

(a) the port operator for the security regulated port; or

(b) the port facility operator for the port facility;

in which the zone is established.

Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.

Subdivision 6.2.3—Cleared zones

6.50 Duties of port facility operator

(1) Immediately after the Secretary gives notice of the establishment of a cleared zone (but before the zone comes into force), the port facility operator for the port facility in which the zone is established must ensure that the zone is inspected for unauthorised persons, goods (including weapons and prohibited items), vehicles and vessels.

(1A) In addition to subregulation (1), if an area is a cleared zone only at certain times, and not continuously, the port facility operator for the port facility in which the zone is established must ensure that the zone is inspected for unauthorised persons, goods (including weapons and prohibited items), vehicles and vessels before each occasion on which the area is a cleared zone.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) A port facility operator must ensure that persons and goods are screened and cleared in accordance with these Regulations before they are allowed to enter and remain in any cleared zone established in the port facility.

6.55 Identification of zones

(1) The boundaries of a cleared zone must be clearly identifiable and defined by means of a security barrier.

(2) Persons who are in or in the vicinity of the security regulated port in which the cleared zone is established must be informed that:
  (a) access to the zone is controlled; and
  (b) any unauthorised entry into the zone is an offence under these Regulations.

6.60 Offences—unauthorised entry

(1) A person who is required to be screened must not enter or remain in a cleared zone unless he or she has been screened and cleared.

  Penalty: 50 penalty units.

(2) A person must not take a vehicle, vessel or thing into, or leave a vehicle, vessel or thing in, a cleared zone unless the vehicle, vessel or thing has been screened and cleared.

  Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.

Subdivision 6.2.4—Water-side restricted zones

6.65 Identification of zones

(1) The boundaries of a water-side restricted zone must be clearly identifiable.

(2) The port operator for the security regulated port in which the water-side restricted zone is established must give notice of the establishment and the boundaries of the water-side restricted zone by:
  (a) water-based identification measures (such as buoys, picket boats and booms); or
  (b) land-side signs; or
  (c) posting, publishing or broadcasting notices; or
  (d) using any other means that have the effect of informing persons in or in the vicinity of the security regulated port about the establishment of the zone and its boundaries.

6.70 Duties of port operator

(1) If the Secretary gives notice of the establishment of a water-side restricted zone, the port operator for the security regulated port in which the water-side restricted

Replaced Authorised Version registered 19/04/2024 F2021C00921

zone is established must ensure that persons who are in, or in the vicinity of, the security regulated port are informed, in accordance with the maritime security plan, that:

(a) access to the zone is controlled; and

(b) any unauthorised entry into the zone is an offence under these Regulations.

(2) The obligation in subregulation (1) has effect even if the zone has not yet come into force.

(3) A port operator for a security regulated port must monitor access to any water-side restricted zone established in the port.

Penalty: 200 penalty units.

(4) An offence against subregulation (3) is an offence of strict liability.

(5) A port operator must ensure that the security measures and procedures to control access to water-side restricted zones detect and deter unauthorised access to those zones.

6.75 Offences—unauthorised entry

(1) A person must not enter or remain in a water-side restricted zone unless authorised to do so by the port operator, or a port facility operator acting on behalf of the port operator, of the security regulated port in which the zone is established.

Penalty: 50 penalty units.

(2) A person must not take a vessel or thing into, or leave a vessel or thing in, a water-side restricted zone unless authorised to do so by the port operator for the security regulated port in which the zone is established.

Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 6.3—Ship security zones

6.80 Exclusion zones

For subsection 107(1) of the Act, an exclusion zone is prescribed as a type of ship security zone.

6.85 Declaration of operation of zone

(1) The port operator for a security regulated port may request the Secretary to declare that a ship security zone is to operate around a security regulated ship while the ship is in the port.

(1A) The offshore facility operator for a security regulated offshore facility may request the Secretary to declare that a ship security zone is to operate around a security regulated ship while the ship is in the vicinity of the offshore facility and is engaged in any activity in relation to the facility.

(2) A request under this regulation must be in writing and must set out:
- (a) the purpose for the proposed declaration; and
- (b) the boundaries of the ship security zone (that is, the distance from the security regulated ship in relation to which access is controlled); and
- (c) the security measures and procedures to be taken to control access into the zone by people, vessels or things; and
- (d) steps to be taken to inform people that a ship security zone has been declared and that entry into the zone without authority is an offence; and
- (e) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (c) and (d).

(3) The Secretary must make a decision on a request made under this regulation.

(4) If the Secretary makes a decision under subregulation (3) to refuse a request, the Secretary must give the person who made the request written notice of the refusal including the reasons for the refusal.

6.90 Identification of zones

(1) The boundaries of a ship security zone must be clearly identifiable.

(2) The relevant operator must give notice of the establishment and the boundaries of the ship security zone by:
- (a) water-based identification measures (such as buoys, picket boats and booms); or
- (b) signs; or
- (c) posting, publishing or broadcasting notices; or
- (d) using any other means that have the effect of informing persons in or in the vicinity of the security regulated port or security regulated offshore facility about the establishment of the zone and its boundaries.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(3) For the purposes of this regulation, ***relevant operator*** means:

(a) the port operator for the security regulated port in which the ship security zone is established; or

(b) the offshore facility operator for the security regulated offshore facility in the vicinity of which the ship security zone is established.

6.95 Duties of port operator

(1) If the Secretary gives notice of the establishment of a ship security zone in a security regulated port, the port operator for the port must ensure that persons who are in, or in the vicinity of, the port are informed, in accordance with the operator's maritime security plan, that:

(a) access to the zone is controlled; and

(b) any unauthorised entry into the zone is an offence under these Regulations.

(2) The obligation in subregulation (1) has effect even if the zone has not yet come into force.

(3) The port operator for a security regulated port must monitor access to any ship security zone established in the port.

Penalty: 200 penalty units.

(4) An offence against subregulation (3) is an offence of strict liability.

(5) The port operator for a security regulated port must ensure that the security measures and procedures to control access to ship security zones detect and deter unauthorised access to those zones.

6.96 Duties of offshore facility operator

(1) If the Secretary gives notice of the establishment of a ship security zone in the vicinity of a security regulated offshore facility, the offshore facility operator for the facility must ensure that persons who are in, or in the vicinity of, the facility are informed, in accordance with the operator's offshore security plan, that:

(a) access to the zone is controlled; and

(b) any unauthorised entry into the zone is an offence under these Regulations.

(2) The obligation in subregulation (1) has effect even if the zone has not yet come into force.

(3) The offshore facility operator for a security regulated offshore facility must monitor access to a ship security zone established in the vicinity of the facility.

Penalty: 200 penalty units.

(4) An offence against subregulation (3) is an offence of strict liability.

(5) The offshore facility operator for a security regulated offshore facility must ensure that the security measures and procedures to control access to a ship

Replaced Authorised Version registered 19/04/2024 F2021C00921

security zone in the vicinity of the facility detect and deter unauthorised access to the zone.

6.100 Offences—unauthorised entry into ship security zone

(1) A person must not enter, or remain in, a ship security zone in a security regulated port unless authorised to do so by the port operator for the port.

Penalty: 50 penalty units.

(2) A person must not enter, or remain in, a ship security zone in the vicinity of a security regulated offshore facility unless authorised to do so by the offshore facility operator for the facility.

Penalty: 50 penalty units.

(3) A person must not take a vessel or thing into, or leave a vessel or thing in, a ship security zone in a security regulated port unless authorised to do so by the port operator for the port.

Penalty: 50 penalty units.

(4) A person must not take a vessel or thing into, or leave a vessel or thing in, a ship security zone in the vicinity of a security regulated offshore facility unless authorised to do so by the offshore facility operator for the facility.

Penalty: 50 penalty units.

(5) An offence against subregulation (1), (2), (3) or (4) is an offence of strict liability.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 6.4—On-board security zones

6.105 On-board restricted areas

For subsection 111(1) of the Act, an on-board restricted area is prescribed as a type of on-board security zone.

6.110 Identification of zones

The boundaries of an on-board security zone established on a regulated Australian ship must be clearly identifiable and must be permanently and sufficiently marked with signs to inform persons who are on board, or in the vicinity of, the ship that:

(a) access to the zone is controlled; and

(b) any unauthorised entry into the zone is an offence under these Regulations.

6.115 Duties of ship operators

(1) A ship operator must monitor and control access to any on-board security zones in a regulated Australian ship.

Penalty: 200 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

(3) A ship operator must ensure that the security measures and procedures to control access to on-board security zones detect and deter unauthorised access to those zones.

6.120 Offences—unauthorised entry

(1) A person must not enter or remain in an on-board security zone unless authorised to do so by the ship operator for the ship on which the zone is established.

Penalty: 50 penalty units.

(2) A person must not take goods or other things into or in an on-board security zone unless authorised to do so by the ship operator for the ship on which the zone is established.

Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 6.5—Offshore security zones

Subdivision 6.5.1—Preliminary

6.125 Types of offshore security zones (Act s 113B)

For subsection 113B(1) of the Act, the following are prescribed as the types of offshore security zones that the Secretary may establish:

(a) offshore facility zone;

(b) offshore water-side zone.

Subdivision 6.5.2—Offshore facility zones

6.130 Identification of zones

(1) An offshore facility zone must be clearly identifiable as an offshore security zone.

(2) Persons who are in or in the vicinity of a zone must be informed that:

(a) access to the zone is controlled; and

(b) any unauthorised entry into the zone is an offence under these Regulations.

6.135 Duties of offshore facility operator

(1) An offshore facility operator must monitor and control access to the offshore facility zone.

Penalty: 200 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

6.140 Offences—unauthorised entry

(1) A person must not enter or remain in an offshore facility zone unless authorised to do so by the offshore facility operator.

Penalty: 50 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

Subdivision 6.5.3—Offshore water-side zones

6.145 Identification of zones

The operator of an offshore facility for which an offshore water-side zone is established must give notice of the establishment and the boundaries of the zone by:

(a) water based identification measures; or

(b) posting, publishing or broadcasting notices; or

Replaced Authorised Version registered 19/04/2024 F2021C00921

(c) using any other means that have the effect of informing persons in or in the vicinity of the zone about the establishment of the zone and its boundaries.

6.150 Duties of offshore facility operator

(1) If the Secretary gives notice of the establishment of an offshore water-side zone, the offshore facility operator concerned must ensure that persons who are in, or in the vicinity of, the security regulated offshore facility are informed, in accordance with the offshore security plan, that:

(a) access to the zone is controlled; and

(b) any unauthorised entry into the zone is an offence under these Regulations.

(2) An offshore facility operator must monitor access to any offshore water-side zone.

Penalty: 200 penalty units

(3) An offence against subregulation (2) is an offence of strict liability.

(4) An offshore facility operator must ensure that the security measures and procedures to control access to offshore water-side zones detect and deter unauthorised access to those zones.

6.155 Offences—unauthorised entry

(1) A person must not enter or remain in an offshore water-side zone unless authorised to do so by the offshore facility operator concerned.

Penalty: 50 penalty units.

(2) A person must not take a vessel or thing into, or leave a vessel or thing in, an offshore water-side zone unless authorised to do so by the offshore facility operator concerned.

Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 7—Other security measures

Division 7.1—Preliminary

7.05 Access not to be denied

(1) Nothing in this Part has the effect of preventing entry into a maritime security zone by a person who:

(a) is accompanied by a law enforcement officer for the purposes of an investigation; or

(b) is an Australian Federal Police employee, a member of the Australian Federal Police, or an officer or employee of the police force or service of a State or Territory, who requires access for the purposes of a police investigation; or

(c) is otherwise authorised by a law of the Commonwealth, State or Territory to enter the maritime security zone.

Example: For paragraph (c), entry to maritime security zones must not be denied to law enforcement officers, customs officers or AMSA officers if the entry is required in the course of their duties.

(2) Nothing in this Part has the effect of preventing a member of the Australian Defence Force who is on duty:

(a) from entering a maritime security zone; or

(b) from taking into a maritime security zone vessels, vehicles or goods:

(i) for the purpose of gaining access to a ship that is under the control, or in the service, of the Australian Defence Force; or

(ii) in connection with the movement, loading, unloading, maintenance or provisioning of such a ship.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 7.2—Screening and clearing

7.20 Duties of port facility operator

The port facility operator for a port facility in which a cleared zone is established must ensure that:

(a) subject to regulation 7.25, persons boarding a security regulated ship that is a passenger ship:
  (i) have been screened in preparation for boarding, and cleared at the time they board the ship; or
  (ii) are screened and cleared immediately after they board the ship; and

(b) subject to regulation 7.27, baggage taken on board the ship:
  (i) has been screened in preparation for being taken on board, and cleared at the time it is taken on board the ship; or
  (ii) is screened and cleared immediately after it is taken on board the ship.

7.25 Persons who need not be screened

(1) For paragraph 115(2)(b) of the Act, the persons mentioned in subregulation (3) may pass through a screening point without being screened when boarding a security regulated ship that is a passenger ship for which maritime security level 1 is in force.

(2) For paragraph 115(2)(c) of the Act, the persons mentioned in subregulation (3) may enter a cleared zone or board a cleared vessel other than through a screening point when maritime security level 1 is in force for the port facility in which the cleared zone is established or in which the cleared vessel is being loaded or unloaded.

(3) For subregulations (1) and (2), the persons are:
  (a) in the case of a security regulated ship that is a passenger ship—a member of the ship's crew; and
  (b) the CSO for the ship, while on duty; and
  (c) the PFSO for the port facility in which the cleared zone is established, while on duty; and
  (d) a PSO for the port in which the cleared zone is established, while on duty; and
  (e) a screening officer; and
  (f) a law enforcement officer; and
  (g) a member of the Australian Defence Force, in the course of his or her duties; and
  (h) an officer of AMSA, in the course of his or her duties; and
  (i) a biosecurity officer, in the course of his or her duties; and
  (j) a member of a fire, ambulance, medical, search or rescue service, in the course of his or her duties; and
  (k) an immigration officer, in the course of his or her duties; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(l) a maritime security inspector, in the course of his or her duties; and

(m) a person appointed by a court to be a Marshal, when exercising a power or function, or performing a duty, conferred or imposed on him or her by the *Admiralty Rules 1988*; and

(n) a person authorised to exercise a power or function, or perform a duty, conferred or imposed on a Marshal under those Rules, when exercising that power or function, or performing that duty.

(4) For paragraph 115(2)(b) of the Act, the following persons may pass through a screening point without being screened when boarding a security regulated ship that is a passenger ship moored at a port facility for which maritime security level 2 or 3 is in force:

(a) a law enforcement officer; and

(b) a member of the Australian Defence Force, in the course of his or her duties; and

(c) a member of a fire, ambulance, medical, search or rescue service, in the course of his or her duties.

7.27 Goods that need not be screened

(1) For paragraph 116(2)(b) of the Act, baggage may pass through a screening point without being screened if the baggage belongs to a person who, under subregulation 7.25(1) or (4), need not be screened when boarding a security regulated ship that is a passenger ship.

(2) For paragraph 116(2)(c) of the Act, baggage and other goods may enter a cleared zone or be taken on board a cleared vessel other than through a screening point if the baggage and goods belong to a person who, under subregulation 7.25(2), may enter the cleared zone or board the cleared vessel other than through the screening point.

7.28 Vehicles that need not be screened

(1) For paragraph 117(2)(b) of the Act, a vehicle may pass through a screening point without being screened if the vehicle is being driven by a member of the Australian Defence Force who, under subregulation 7.25(1) or (4), need not be screened when boarding a security regulated ship that is a passenger ship.

(2) For paragraph 117(2)(c) of the Act, a vehicle may enter a cleared zone or go on board a cleared vessel other than through a screening point if the vehicle is being driven by a member of the Australian Defence Force who, under subregulation 7.25(2), may enter the cleared zone or board the cleared vessel other than through the screening point.

7.29 Vessels that need not be screened

(1) For paragraph 118(2)(b) of the Act, a vessel may pass through a screening point without being screened if the vessel is under the control of a member of the

Replaced Authorised Version registered 19/04/2024 F2021C00921

Australian Defence Force who, under subregulation 7.25(1) or (4), need not be screened when boarding a security regulated ship that is a passenger ship.

(2) For paragraph 118(2)(c) of the Act, a vessel may enter a cleared zone or be taken on board a cleared vessel other than through a screening point if the vessel is under the control of a member of the Australian Defence Force who, under subregulation 7.25(2), may enter the cleared zone or board the cleared vessel other than through the screening point.

7.30 Methods, techniques and equipment to be used for screening—Secretary's notice

(1) For subsection 119(3) of the Act, the Secretary may, by written notice, state 1 or more of the following:

(a) the method to be used for screening under this Part;

(b) the technique to be used for screening under this Part;

(c) the equipment to be used for screening under this Part.

Note: The notice may provide that the notice is to be given only to the person, or class of persons, specified in the notice—see subsection 119(3) of the Act.

(1A) To avoid doubt, and without limiting subregulation (1), a notice under that subregulation may apply in relation to a large passenger ship or a small passenger ship.

(2) A notice under subregulation (1) is binding on a person only if it has been served on the person.

7.31 Equipment to be used for screening—no notice

(1) This regulation applies if there is no notice in force under regulation 7.30 stating the equipment to be used for screening under this Part.

(2) For subsection 119(1) of the Act, the equipment to be used for screening under this Part must be capable of detecting prohibited items and weapons on persons or in baggage.

Note: For the meaning of ***prohibited item*** and ***weapon***, see section 10 of the Act and regulations 1.60 and 1.65.

(3) The equipment may comprise a combination of screening equipment such as a walk-through metal detector, hand-held metal detector, trace explosive detection device and x-ray equipment.

7.33 Notice to be displayed at screening points

(1) For paragraph 119(2)(l) of the Act, notices that it is an offence under the Act to carry weapons or prohibited items through a screening point must be displayed with reasonable prominence at screening points.

(2) A notice must include a list of weapons and prohibited items for the purposes of the Act.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Note 1: See section 10 of the Act and regulations 1.60 and 1.65 as to what are prohibited items and weapons.

Note 2: Sections 121 and 128 of the Act create the offences of carrying weapons and prohibited items through screening points. Certain persons are authorised, under those sections and regulation 7.45, to carry weapons or prohibited items through screening points.

7.34 Supervision and control measures to ensure persons and baggage remain cleared

For paragraph 119(2)(m) of the Act, either or both of the following are supervision and control measures to ensure that a person or baggage that has received clearance remains cleared on a vessel that is not a cleared vessel or in an area that is not a cleared area:

(a) the person or baggage is continuously supervised by security personnel while on the vessel or in the area;

(b) the person or baggage is continuously monitored by security personnel through closed circuit television while on the vessel or in the area.

Note: Subsections 115(4) and 116(4) of the Act provide that a person is, or goods are, taken to be in a cleared area if the person is, or goods are, under the supervision or control prescribed in the regulations.

7.35 Offences—screening and clearing

(1) A port facility operator must not allow a person who is required to be screened to enter a cleared zone, unless the person has been screened and cleared.

Penalty: 200 penalty units.

(2) A port facility operator must not allow goods that are required to be screened to enter a cleared zone, unless the goods have been screened and cleared.

Penalty: 200 penalty units.

(3) A port facility operator must not allow a person who is required to be screened and cleared to board a security regulated ship that is a passenger ship that is moored at the facility, unless:

(a) if there is a screening point through which the person must pass at the facility—the person has been screened in preparation for boarding, and cleared at the time the person boards the ship;

(b) if there is no such screening point at the facility—the port facility operator has made arrangements with the master of the ship for the person to be screened and cleared on board the ship immediately after the person boards the ship.

Penalty: 200 penalty units.

(4) A port facility operator must not allow baggage that is required to be screened and cleared to be taken on board a security regulated ship that is a passenger ship that is moored at the facility, unless:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(a) if there is a screening point through which the baggage must pass at the facility—the baggage has been screened in preparation for being taken on board the ship, and cleared at the time it is taken on board;

(b) if there is no such screening point at the facility—the port facility operator has made arrangements with the master of the ship for the baggage to be screened and cleared on board the ship immediately after the baggage is taken on board.

Penalty: 200 penalty units.

(5) A ship operator for a security regulated ship that is a passenger ship must not allow a person who is required to receive clearance to board the ship, unless:

(a) the person is cleared at the time the person boards the ship; or

(b) the person is screened and cleared on board the ship immediately after the person boards the ship.

Penalty: 200 penalty units.

(6) A ship operator for a security regulated ship that is a passenger ship must not allow baggage that is required to receive clearance to be taken on board the ship, unless:

(a) the baggage is cleared at the time it is taken on board the ship; or

(b) the baggage is screened and cleared on board the ship immediately after the baggage is taken on board.

Penalty: 200 penalty units.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 7.3—Weapons and prohibited items

7.39 Definition of *licensed security guard* for Division 7.3

(1) In this Division:

licensed security guard means a person who holds a licence to work as a security guard, being a licence:

(a) issued or recognised by the State or Territory in which the person is working; and

(b) that is in force.

(2) For the purposes of paragraph (a) of the definition of ***licensed security guard*** in subregulation (1), if a person is working outside of a State or Territory on a regulated Australian ship or a regulated offshore facility, the person is taken to be working in:

(a) for a regulated Australian ship—the State or Territory in which the ship's home port (within the meaning of the *Shipping Registration Regulations 1981*) is located; or

(b) for a regulated offshore facility—the State or Territory adjacent to the place where the offshore facility is located.

7.40 Persons authorised to possess weapons or prohibited items in maritime security zones

(1) This regulation applies for sections 120 and 127 of the Act.

(2) A person is authorised to have a weapon or prohibited item in his or her possession while in a maritime security zone if the person is:

(a) a maritime security guard, an SSO, or a licensed security guard, who is on duty; or

(b) the master of a security regulated ship located in the zone who has the weapon or prohibited item in his or her possession for the purpose of securing it for carriage on board the ship; or

(c) a PSO, PFSO or screening officer, who has the weapon or prohibited item in his or her possession for the purpose of securing it for carriage on board a security regulated ship; or

(d) a veterinarian, or a biosecurity officer, who has the weapon or prohibited item in his or her possession for the purpose of controlling or euthanasing animals in a maritime security zone or on board a security regulated ship or other vessel; or

(e) a biosecurity officer who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases in a maritime security zone or on board a security regulated ship or other vessel; or

(f) an officer of a State or Territory department who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests

Replaced Authorised Version registered 19/04/2024 F2021C00921

or treating diseases in a maritime security zone, or on board a security regulated ship or other vessel, under a law of the State or Territory.

(3) In addition, a person is authorised to have a weapon or prohibited item in his or her possession while in a maritime security zone if:

(a) the person is:

(i) an inspector of the Royal Society for the Prevention of Cruelty to Animals of a State or Territory; or

(ii) an officer of any other organisation that has as one of its objects the promotion of the welfare of, or the prevention of cruelty to, animals; and

(b) the person has the weapon or prohibited item in his or her possession in connection with carrying out an inspection related to the welfare of any animals in a maritime security zone or on board a security regulated ship; and

(c) the inspection is authorised by a law of the State or Territory in which the maritime security zone or the ship is located.

7.45 Authorised possession of weapons or prohibited items when passing through screening points

(1) This regulation applies for sections 121 and 128 of the Act.

(2) A person is authorised to pass through a screening point with a weapon or prohibited item in his or her possession if the person is:

(a) a maritime security guard, an SSO, or a licensed security guard, who is on duty; or

(b) the master of a security regulated ship who is passing through the screening point with the weapon or prohibited item in his or her possession for the purpose of securing it for carriage on board the ship; or

(c) a PSO, PFSO or screening officer, who is passing through the screening point with the weapon or prohibited item in his or her possession for the purpose of securing it for carriage on board a security regulated ship; or

(d) an ADF member who is on duty; or

(e) a veterinarian, or a biosecurity officer, who has the weapon or prohibited item in his or her possession for the purpose of controlling or euthanasing animals in a maritime security zone or on board a security regulated ship; or

(f) a biosecurity officer who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases in a maritime security zone or on board a security regulated ship; or

(g) an officer of a State or Territory department who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases in a maritime security zone, or on board a security regulated ship, under a law of the State or Territory.

(3) In addition, a person is authorised to pass through a screening point with a weapon or prohibited item in his or her possession if:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(a) the person is:
(i) an inspector of the Royal Society for the Prevention of Cruelty to Animals of a State or Territory; or
(ii) an officer of any other organisation that has as one of its objects the promotion of the welfare of, or the prevention of cruelty to, animals; and
(b) the person has the weapon or prohibited item in his or her possession in connection with carrying out an inspection related to the welfare of any animals in a maritime security zone or on board a security regulated ship; and
(c) the inspection is authorised by a law of the State or Territory in which the maritime security zone or the ship is located.

7.50 Authorised carriage or possession of weapons or prohibited items on board regulated Australian ships

(1) This regulation applies for sections 122, 123, 129 and 130 of the Act.

(2) A person is authorised to carry, or otherwise have in his or her possession, a weapon or prohibited item on board a regulated Australian ship if the person is:
(a) a maritime security guard, an SSO, or a licensed security guard, who is on duty; or
(b) the master of the ship, or a PSO, PFSO or screening officer, who has the weapon or prohibited item in his or her possession for the purpose of securing the weapon or prohibited item for carriage on the ship; or
(c) an ADF member who is on duty; or
(d) a veterinarian, or a biosecurity officer, who has the weapon or prohibited item in his or her possession for the purpose of controlling or euthanasing animals on board the ship; or
(e) a biosecurity officer who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases on board the ship; or
(f) an officer of a State or Territory department who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases on board the ship under a law of the State or Territory.

(3) In addition, a person is authorised to carry, or otherwise have in his or her possession, a weapon or prohibited item on board a regulated Australian ship if:
(a) the person is:
(i) an inspector of the Royal Society for the Prevention of Cruelty to Animals of a State or Territory; or
(ii) an officer of any other organisation that has as one of its objects the promotion of the welfare of, or the prevention of cruelty to, animals; and
(b) the person has the weapon or prohibited item in his or her possession in connection with carrying out an inspection related to the welfare of any animals on board the ship; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(c) the inspection is authorised by a law of the State or Territory in which the ship is located.

7.55 Authorisation subject to compliance with other laws

In spite of regulations 7.40, 7.45 and 7.50, a person is not authorised to carry or possess a weapon or prohibited item in the circumstances stated in those regulations if:

(a) carriage or possession of the weapon or prohibited item is prohibited by another law of the Commonwealth, or a law of a State or Territory, without a licence, permit or authorisation; and

(b) the person does not have a licence, permit or authorisation of that kind for the weapon or prohibited item.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 8—Powers of officials

Division 8.1—Preliminary

Note: This Division heading is reserved for future use.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 8.2—Maritime security inspectors

8.20A Maritime security inspectors—criteria for appointment

(1) For paragraph 136(1)(c) of the Act, the Secretary may appoint a person to be a maritime security inspector if the Secretary is satisfied that:

(a) the person:

(i) is an IRCA certificated auditor; or

(ii) has qualifications that are equivalent to those that an IRCA certificated auditor has; or

(iii) has experience that is equivalent to the experience that an IRCA certificated auditor has; and

(b) the person:

(i) has a working knowledge of the Act and these Regulations, including the powers, functions and duties of a maritime security inspector; and

(ii) is a suitable person to access and handle security information; and

(iii) is otherwise able to perform the duties of a maritime security inspector.

(2) In this regulation:

IRCA certificated auditor means an auditor who is certified by the International Register of Certificated Auditors.

8.20 Identity cards (Act s 137(2))

(1) The minimum requirements in relation to the form of an identity card for a maritime security inspector are as follows:

(a) the card must bear a recent photograph of the holder;

(b) the card must set out the holder's name;

(c) the card must bear a statement of its date of expiry;

(d) the card must bear a statement to the effect that the holder is a maritime security inspector appointed under section 136 of the Act;

(e) the card must bear the signatures of the holder and the Secretary.

(2) If a person representing or apparently representing a maritime industry participant so requests, a maritime security inspector must show his or her identity card to the person.

Penalty: 5 penalty units.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 8.2A—Security assessment inspectors

8.25 Security assessment inspectors—criteria for appointment

For subsection 145D(1) of the Act, the criteria are:

(a) the person is:

(i) an APS employee in the Department; or

(ii) a member of the Australian Federal Police; or

(iii) a member of the police force of a State or a Territory; or

(iv) a customs officer; or

(b) the person:

(i) has a good knowledge of the transport security environment; and

(ii) has skills, experience or qualifications relevant to conduct a security assessment; and

(iii) has a working knowledge, or the ability to acquire a working knowledge, of the Act and these Regulations; and

(iv) is suitable to access and handle security information; and

(v) is otherwise able to perform the duties of a security assessment inspector.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 8.3—Duly authorised officers

Note: This Division heading is reserved for future use.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 8.4—Law enforcement officers

8.40 Customs officers who are law enforcement officers

For paragraph (c) of the definition of ***law enforcement officer*** in section 151 of the Act, the following are prescribed:

(a) customs officers who are covered by paragraph (a) of the definition of ***Immigration and Border Protection worker*** in subsection 4(1) of the *Australian Border Force Act 2015* and who are in the Australian Border Force (within the meaning of that Act);

(b) customs officers who are assigned customs duties associated with:

(i) intelligence activities; or

(ii) passenger processing; or

(iii) compliance, investigation or enforcement of border and cargo matters.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 8.5—Maritime security guards

Subdivision 8.5.1—Maritime security guards—general

8.50 Training and qualifications

(1) For the purposes of paragraph 162(2)(a) of the Act, the following are prescribed as training and qualification requirements for maritime security guards:

(a) the person:

(i) must hold at least a Certificate II in Security Operations that is in force; or

(ii) must hold a certificate or qualification that is in force and that is equivalent to at least a Certificate II in Security Operations (for example, a Certificate II in Security (Guarding)); or

(iii) must have undergone training and acquired experience while working as a security guard that is sufficient to satisfy the requirements for obtaining a security guard licence in a State or Territory;

(b) the person must hold a licence to work as a security guard, being a licence:

(i) issued or recognised by the State or Territory in which the person is working; and

(ii) that is in force;

(c) the person must have a working knowledge of the Act and these Regulations, including knowledge about how to restrain and detain persons in accordance with section 163 of the Act.

(2) For the purposes of subparagraph (1)(b)(i), if a person is working outside of a State or Territory on a regulated Australian ship or a regulated offshore facility, the person is taken to be working in:

(a) for a regulated Australian ship—the State or Territory in which the ship's home port (within the meaning of the *Shipping Registration Regulations 1981*) is located; or

(b) for a regulated offshore facility—the State or Territory adjacent to the place where the offshore facility is located.

8.55 Identity cards (Act s 162(2)(b))

(1) The requirements in relation to the issue and use of an identity card for a maritime security guard are as follows:

(a) the card must be:

(i) issued to the maritime security guard by his or her employer; or

(ii) issued by an authority of a State or Territory, and be evidence that the maritime security guard holds a licence to work as a security guard in that State or Territory;

(b) the card must be displayed by the maritime security guard while he or she is on duty.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) The minimum requirements in relation to the form of the identity card are as follows:

(a) the card must bear a recent photograph of the maritime security guard;

(b) the card must set out the guard's name;

(c) the card must bear a statement of its date of expiry;

(d) the card must bear:

(i) the name of the employer that issued the card; or

(ii) if the card is issued by an authority of a State or Territory—the name of the authority.

Subdivision 8.5.2—Removal and disposal of vehicles and vessels from zones

8.57 Disposal of removed vehicles (Act s 163D)

(1) For this regulation, a vehicle is an ***unclaimed vehicle*** if:

(a) the vehicle has been removed from a maritime security zone under section 163D of the Act; and

(b) the owner of the vehicle has not claimed the vehicle and paid any costs or expenses in relation to the vehicle's removal, relocation and storage.

(2) If a vehicle has been an unclaimed vehicle for longer than 3 months, the maritime industry participant that controls the maritime security zone from which the vehicle was removed may sell or otherwise dispose of the vehicle as provided in this regulation.

(3) Not less than 3 months after the vehicle was removed from the zone, the participant must publish a notice in a newspaper circulating generally in the State or Territory in which the zone is located:

(a) describing the vehicle and the place and zone from which it was removed; and

(b) stating that:

(i) the vehicle has been removed, relocated or stored (as the case may be); and

(ii) the owner must pay the costs of removal, relocation or storage to the participant; and

(iii) if the costs are not paid within 14 days of the publication, the vehicle may be sold or otherwise disposed of; and

(c) setting out how the costs may be paid.

(4) If, more than 14 days after the publication of the notice, the owner of the vehicle has not:

(a) recovered the vehicle; and

(b) paid to the participant an amount equal to the costs of the vehicle's removal, relocation or storage to the participant;

the participant:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(c) if the vehicle is saleable—must sell the vehicle at a price that is reasonable under the circumstances; or

(d) otherwise—may dispose of the vehicle by another means.

(5) If the vehicle is sold:

(a) the participant may retain from the sale proceeds an amount equal to the reasonable costs of removal, relocation or storage of the vehicle; and

(b) any amount of the proceeds remaining after the retention is a debt due to the Commonwealth, payable by 14 July immediately following the financial year in which the vehicle was sold.

8.58 Disposal of removed vessels (Act s 163E)

(1) For this regulation, a vessel is an ***unclaimed vessel*** if:

(a) the vessel has been removed from a maritime security zone under section 163E of the Act; and

(b) the owner of the vessel has not claimed the vessel and paid any costs or expenses in relation to the vessel's removal, relocation and storage.

(2) If a vessel has been an unclaimed vessel for longer than 3 months, the maritime industry participant that controls the maritime security zone from which the vessel was removed may sell or otherwise dispose of the vessel as provided in this regulation.

(3) Not less than 3 months after the vessel was removed from the zone, the participant must publish a notice in a newspaper circulating generally in the State or Territory in which the zone is located:

(a) describing the vessel and the place and zone from which it was removed; and

(b) stating that:

(i) the vessel has been removed, relocated or stored (as the case may be); and

(ii) the owner must pay the costs of removal, relocation or storage to the participant; and

(iii) if the costs are not paid within 14 days of the publication, the vessel may be sold or otherwise disposed of; and

(c) setting out how the costs may be paid.

(4) If, more than 14 days after the publication of the notice, the owner of the vessel has not:

(a) recovered the vessel; and

(b) paid to the participant an amount equal to the costs of the vessel's removal, relocation or storage to the participant;

the participant:

(c) if the vessel is saleable—must sell the vessel at a price that is reasonable under the circumstances; or

(d) otherwise—may dispose of the vessel by another means.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(5) If the vessel is sold:

(a) the participant may retain from the sale proceeds an amount equal to the reasonable costs of removal, relocation or storage of the vessel; and

(b) any amount of the proceeds remaining after the retention is a debt due to the Commonwealth, payable by 14 July immediately following the financial year in which the vessel was sold.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 9—Reporting maritime transport or offshore facility security incidents

Note: This Part heading is reserved for future use.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 10—Information-gathering

Note: This Part heading is reserved for future use.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 11—Enforcement

Division 11.2—Infringement notices

11.05 Purpose and effect of Division

(1) The purpose of this Division is to create a system of infringement notices for certain offences against the Act and these Regulations as an alternative to prosecution.

(2) This Division does not:
  (a) require an infringement notice to be issued to a person for an offence; or
  (b) affect the liability of a person to be prosecuted for an offence if an infringement notice is not issued to the person for the offence; or
  (c) prevent the issue of 2 or more infringement notices to a person for an offence; or
  (d) affect the liability of a person to be prosecuted for an offence if the person does not comply with an infringement notice for the offence; or
  (e) limit or otherwise affect the penalty that may be imposed by a court on a person convicted of an offence.

11.10 Definition for Division—*authorised person*

In this Division:

authorised person means:
  (a) a law enforcement officer; or
  (b) a maritime security inspector.

11.15 Amount of penalty if infringement notice issued

The penalty for an offence payable under an infringement notice issued to a person for the offence is one-fifth of the maximum penalty that a court could impose on the person for the offence.

11.20 Authorised persons may issue infringement notices

(1) In this regulation:

infringement notice offence means an offence:
  (a) against any provision of the Act (other than subsection 43(1), 62(1) or 100C(1)) a contravention of which is an offence of strict liability; or
  (b) against a provision of these Regulations (being an offence that is an offence of strict liability).

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) If an authorised person has reason to believe that a person has committed an infringement notice offence, the authorised person may issue a notice (called an infringement notice) to the person for the offence.

11.25 Contents of infringement notice

(1) An infringement notice:

(a) must bear a unique number; and

(b) must state the name of the authorised person who issued it, and:

(i) if he or she is a law enforcement officer (other than a customs officer)—the name of the police force or police service of which he or she is a member; or

(ii) if he or she is a customs officer or a maritime security inspector—that fact; and

(c) must state its date of issue; and

(d) must state the full name, or the surname and initials, and the address, of the person to whom it is issued; and

(e) must give brief details of the alleged offence for which it is issued, including:

(i) the date and time of the offence; and

(ii) where the offence happened; and

(iii) the provision of the Act or these Regulations contravened; and

(f) must state the penalty for the offence payable under the notice; and

(g) must state where and how that penalty can be paid (including, if the penalty can be paid by posting the payment, the place to which it should be posted); and

(h) must state that if the person to whom it is issued (the ***recipient***) pays the penalty within 28 days after the day when the notice is served (or any longer time allowed in writing by the Secretary), then:

(i) any liability of the recipient for the offence will be discharged; and

(ii) the recipient will not be prosecuted in a court for the offence; and

(iii) the recipient will not be taken to have been convicted of the offence; and

(i) must state the greatest penalty that a court could impose on the recipient for the offence; and

(j) must state the number of demerit points that the recipient will accrue for the offence; and

(k) must state that if the recipient is prosecuted in court and found guilty of the offence:

(i) the recipient may be convicted of the offence and ordered to pay a penalty and costs; and

(ii) will be subject to any other order that the court makes; and

(iii) will accrue the number of demerit points specified in the notice; and

(l) must state how and to whom the recipient can apply to be allowed more time to pay the penalty; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(m) must be signed by the authorised person who issued it.

(2) An infringement notice may contain any other information that the authorised person who issues it thinks necessary.

11.30 Service of infringement notices

(1) An infringement notice must be served on the person to whom it is issued.

(2) An infringement notice may be served on an individual:
(a) by giving it to the individual; or
(b) by leaving it at, or by sending it by post, telex, fax or similar facility to, the address of the place of residence or business (the ***relevant place***) of the individual last known to the authorised person who issues it; or
(c) by giving it, at the relevant place, to someone who:
(i) lives or is employed, or apparently lives or is employed, there; and
(ii) is, or the authorised person who issues it has reason to believe is, over 16 years of age.

(3) An infringement notice may be served on a corporation:
(a) by leaving it at, or by sending it by post, telex, fax or similar facility to, the address of the head office, a registered office or a principal office of the corporation; or
(b) by giving it, at an office mentioned in paragraph (a), to someone who is, or the authorised person who issues it has reason to believe is, an officer or employee of the corporation.

11.35 Time for payment of penalty

The penalty stated in an infringement notice must be paid:
(a) within 28 days after the day on which the notice is served on the person to whom it is issued; or
(b) if the person applies for a further period of time in which to pay the penalty, and that application is granted—within the further period allowed; or
(c) if the person applies for a further period of time in which to pay the penalty, and the application is refused—within 7 days after the notice of the refusal is served on the person; or
(d) if the person applies for the notice to be withdrawn, and the application is refused—within 28 days after the notice of the refusal is served on the person.

11.40 Extension of time to pay penalty

(1) The person to whom an infringement notice is issued (the ***recipient***) may apply, in writing, to the Secretary for a further period of up to 28 days in which to pay the penalty stated in the notice.

(2) Within 14 days after receiving the application, the Secretary:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(a) must grant or refuse a further period not longer than the period sought; and
(b) must notify the recipient in writing of the decision and, if the decision is a refusal, the reasons for it.

(3) Notice of the decision may be served on the recipient in any way in which the infringement notice could have been served on the recipient.

11.45 Payment of penalty

(1) An infringement notice penalty is not paid until the whole of the amount of the penalty has been received by the Commonwealth.

(2) In particular, if the Commonwealth accepts a cheque in payment of a penalty or part of a penalty, the penalty is not paid until the cheque has been honoured.

11.50 Effect of payment of penalty

(1) If the person to whom an infringement notice is issued for an offence pays the penalty stated in the notice:
(a) any liability of the person for the offence is discharged; and
(b) the person may not be prosecuted in a court for the offence; and
(c) the person is not taken to have been convicted of the offence.

(2) If 2 or more infringement notices are issued to a person for the same offence, the person's liability to be prosecuted for the offence ceases if the person pays the penalty stated in any of the notices.

11.55 Withdrawal of infringement notice

(1) Before the end of 28 days after receiving an infringement notice, a person may apply, in writing, to the Secretary for the infringement notice to be withdrawn.

(2) The application must set out the facts or matters that the person believes the Secretary should take into account in relation to the offence alleged in the infringement notice.

(3) Within 14 days after receiving the application, the Secretary must:
(a) withdraw or refuse to withdraw the notice; and
(b) notify the person in writing of the decision and, if the decision is a refusal, the reasons for the decision.

(4) If the Secretary has not approved, or refused to approve, the withdrawal of the notice within the period allowed by subregulation (3), the Secretary is taken to have refused to approve the withdrawal of the notice.

(5) Before withdrawing or refusing to withdraw a notice, the Secretary must consider:
(a) whether the person has been convicted previously of an offence against the Act or these Regulations; and
(b) the circumstances of the offence stated in the notice; and

Replaced Authorised Version registered 19/04/2024 F2021C00921

(c) whether the person has previously paid a penalty under an infringement notice issued to the person for an offence of the same type as the offence mentioned in the notice; and

(d) any other relevant matter.

(6) The Secretary may also withdraw an infringement notice on his or her own initiative.

11.60 Notice of withdrawal of infringement notices

(1) Notice of the withdrawal of an infringement notice may be served on a person in any way in which the infringement notice could have been served on the person.

(2) A notice withdrawing an infringement notice:

(a) must include the following information:

(i) the full name, or surname and initials, and address of the person on whom the infringement notice was served;

(ii) the number of the infringement notice;

(iii) the date of issue of the infringement notice; and

(b) must state that the notice is withdrawn; and

(c) if the Secretary intends to prosecute the person in a court for the relevant offence, must state that the person may be prosecuted in a court for the offence.

11.65 Refund of penalty etc if infringement notice withdrawn

(1) If an infringement notice is withdrawn after the penalty stated in it has been paid:

(a) the Commonwealth must refund the amount of the penalty to the person who paid it; and

(b) any demerit points accrued because of the payment are cancelled.

(2) If the cancelled demerit points had been accumulated in respect of a ship, the number of demerit points accumulated in respect of the ship decreases by that number of demerit points.

11.70 Evidence of certain matters in relation to infringement notices

(1) At the hearing of a prosecution for an offence in relation to which an infringement notice has been issued, a certificate of any of the following kinds, signed by or on behalf of the Secretary, is evidence of the facts stated in it:

(a) a certificate stating that:

(i) the infringement notice was served on the alleged offender; and

(ii) the infringement notice penalty has not been paid in accordance with this Division;

(b) a certificate stating that the notice was withdrawn on a day specified in the certificate;

(c) a certificate stating that:

Replaced Authorised Version registered 19/04/2024 F2021C00921

(i) a further period was refused for payment of the infringement notice penalty; and

(ii) the infringement notice penalty has not been paid in accordance with this Division;

(d) a certificate stating that:

(i) the further time mentioned in the certificate for payment of the infringement notice penalty was granted; and

(ii) the infringement notice penalty was not paid in accordance with the notice or within the further time.

(2) A certificate that purports to have been signed by or on behalf of the Secretary is presumed to have been so signed unless the contrary is proved.

11.75 Effect of certain admissions

Evidence of an admission made by a person in an application under regulation 11.55 is not admissible in proceedings against the person for the relevant alleged offence unless the person introduces the application into evidence.

11.80 Matter not to be taken into account in determining sentence

If a person to whom an infringement notice has been issued:

(a) does not pay the infringement notice penalty; and

(b) is prosecuted for, and convicted of, the alleged offence mentioned in the infringement notice;

the court must not, in determining the penalty to be imposed, take into account the fact that the person did not pay the infringement notice penalty.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Division 11.6—Demerit points system

11.300 Purpose of Division

This Division establishes a demerit points system under which the approval of a maritime security plan, a ship security plan or an offshore security plan may be cancelled.

11.305 Accrual of demerit points by maritime industry participants

(1) If a maritime industry participant:

(a) is issued with an infringement notice, and pays the infringement notice penalty; or

(b) is convicted or found guilty of an offence;

the participant accrues 1 demerit point for each penalty unit of:

(c) the maximum number of penalty units that a court could impose on the participant for the alleged offence; or

(d) if the penalty for the offence is a term of imprisonment—the maximum number of penalty units that the court could impose in lieu of imprisonment.

(2) To avoid doubt, a reference in subregulation (1) to the maximum number of penalty units that a court could impose is, if the alleged offender is a corporation, the maximum number that the court could impose taking into account subsection 4B(3) of the *Crimes Act 1914*.

11.310 Accumulation of demerit points in respect of ships

Demerit points are accumulated in respect of a ship only if a ship operator accrues the demerit points because the operator:

(a) has been convicted or found guilty of an offence against section 62 or 63 of the Act in respect of the ship; or

(b) has been issued with an infringement notice for an offence against section 63 of the Act in respect of the ship, and has paid the infringement notice penalty as an alternative to prosecution.

11.315 Expiry of demerit points

A demerit point expires 5 years after it is accrued.

11.320 Demerit points—maritime security plans

For section 199 of the Act, the approval of the maritime security plan of a maritime industry participant may be cancelled if the participant accrues:

(a) in the case of a maritime industry participant who is an individual—600 demerit points; or

(b) in any other case—3 000 demerit points.

Replaced Authorised Version registered 19/04/2024 F2021C00921

11.325 Demerit points—ship security plans

For section 200 of the Act, the approval of a ship security plan may be cancelled if 3 000 demerit points are accumulated in respect of the ship.

11.330 Demerit points—offshore security plans

For section 200A of the Act, the approval of the offshore security plan of an offshore industry participant may be cancelled if the participant accrues:

(a) in the case of an offshore industry participant who is an individual—600 demerit points; or

(b) in any other case—3 000 demerit points.

11.335 Register of demerit points

(1) The Secretary must keep a register of demerit points accrued.

(2) The register may be kept by means of, or partly by means of, a computer system.

(3) The register must record, for each maritime industry participant:

(a) for each offence against the Act or these Regulations of which the participant has been convicted or found guilty:

(i) the number of demerit points accrued for the offence; and

(ii) the basis on which the number of demerit points was calculated; and

(iii) the dates on which those demerit points were accrued, and will expire; and

(iv) whether the demerit points were accumulated in respect of a ship and if so what ship; and

(b) for each alleged offence against the Act or these Regulations for which an infringement notice has been issued to the participant, and for which the participant has paid the infringement notice penalty:

(i) the number of demerit points accrued for the alleged offence; and

(ii) the basis on which the number of demerit points was calculated; and

(iii) the dates on which those demerit points were accrued, and will expire; and

(iv) whether the demerit points were accumulated in respect of a ship and if so what ship; and

(c) the total number of demerit points, other than demerit points that have expired, that the participant has accrued.

(4) The register must also record, for each ship in respect of which demerit points have been accumulated:

(a) a reference to the record in the register of each relevant accrual of demerit points by a maritime industry participant; and

(b) the total number of demerit points, other than demerit points that have expired, accumulated in respect of the ship.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Regulation 11.335

(5) The Secretary must allow a maritime industry participant, at a reasonable time and on reasonable notice, to inspect the record of the participant's accrued demerit points.

(6) The Secretary must allow a ship operator, at a reasonable time and on reasonable notice, to inspect the record of demerit points accumulated in respect of a ship operated by the operator.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 12—Review of decisions

12.01 Review of decisions by Administrative Appeals Tribunal

Application may be made to the Administrative Appeals Tribunal for a review of a decision made by the Secretary under subregulation 6.85(3) not to declare that a ship security zone is to operate around a security regulated ship.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 13—Miscellaneous

13.05 Ship security alert systems

(1) A regulated Australian ship must be provided with a ship security alert system:

(a) for a ship constructed on or after 1 July 2004—before registration of the ship under the *Shipping Registration Act 1981*; and

(b) for a passenger ship (including a high-speed passenger craft) constructed before 1 July 2004—not later than the first survey of the ship's radio installation after 1 July 2004; and

(c) for an oil tanker, chemical tanker, gas carrier, bulk carrier or a cargo high speed craft, 500 gross tonnage or more, constructed before 1 July 2004—not later than the first survey of the ship's radio installation after 1 July 2004; and

(d) for any other cargo ship 500 gross tonnage or more or mobile offshore drilling unit constructed before 1 July 2004—not later than the first survey of the ship's radio installation after 1 July 2006.

(2) A ship security alert:

(a) must be capable of transmitting a ship-to-shore security alert identifying the ship, giving its location and indicating that the security of the ship is, or was, under threat; and

(b) must otherwise comply with regulation XI-2/6 of the SOLAS Convention.

Note: For the definition of ***SOLAS Convention***, see section 10 of the Act.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 14—Transitional arrangements

14.01 Operation of Schedule 2

Schedule 2 makes transitional arrangements in relation to amendments of these Regulations.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Schedule 1—Maritime-security-relevant offences

Note: See the definitions of ***maritime-security-relevant offence***, ***tier 1 offence***, ***tier 2 offence*** and ***tier 3 offence*** in subregulation 6.07B(1).

1 Tier 1 offences

The following table lists offences that are tier 1 maritime-security-relevant offences.

Maritime-security-relevant offences—tier 1 offences

Item	Offence
1	An offence involving terrorism
2	An offence involving treason, advocating terrorism or genocide, or urging violence
3	An offence involving espionage or selling national secrets
4	An offence relating to engagement in hostile activities in a foreign country or involvement with foreign armed forces
5	An offence relating to weapons of mass destruction
6	An offence involving hijacking or destroying an aircraft, vessel or offshore facility that is used in commerce or owned by the government
7	An offence involving endangerment of an aircraft, airport, vessel, port or offshore facility that is used in commerce or owned by the government
8	An offence involving an act of piracy at sea
9	An offence relating to involvement with a criminal organisation or gang
10	An offence involving the smuggling or trafficking of people

Note: A person convicted of an offence mentioned in the table will have an adverse criminal record (see the definition of ***adverse criminal record*** in subregulation 6.07B(3)).

2 Tier 2 offences

The following table lists offences that are tier 2 maritime-security-relevant offences.

Maritime-security-relevant offences—tier 2 offences

Item	Offence
1	An offence relating to assaulting or threatening a person on an aircraft, vessel or offshore facility, or in an airport or port
2	An offence relating to theft of an aircraft or vessel that is used in commerce or owned by the government
3	An offence relating to questioning conducted by a person or body investigating serious crime or corruption
4	An offence under the Act that is punishable by imprisonment (whether or not the person is in fact sentenced to imprisonment)

Replaced Authorised Version registered 19/04/2024 F2021C00921

Maritime-security-relevant offences—tier 2 offences	
Item	**Offence**
5	An offence under the *Aviation Transport Security Act 2004* that is punishable by imprisonment (whether or not the person is in fact sentenced to imprisonment)

Note: A person convicted of an offence mentioned in the table will have an adverse criminal record (see the definition of ***adverse criminal record*** in subregulation 6.07B(3)).

3 Tier 3 offences

The following table lists offences that are tier 3 maritime-security-relevant offences.

Maritime-security-relevant offences—tier 3 offences	
Item	**Offence**
1	Murder or manslaughter
2	An offence relating to false imprisonment, deprivation of liberty or taking a hostage
3	An offence relating to assault (other than offences referred to in clauses 1 and 2 of this Schedule), including indecent or sexual assault
4	An offence relating to the sexual abuse or sexual exploitation of a child
5	An offence relating to intimidation (other than offences referred to in clauses 1 and 2 of this Schedule)
6	An offence relating to endangerment of others (other than offences referred to in clauses 1 and 2 of this Schedule), but not including traffic offences except where a vehicle is used as a weapon
7	An offence relating to affray or riot
8	An offence relating to assaulting or resisting a law enforcement officer or other public officer
9	An offence of impersonating a law enforcement officer or other public officer
10	An offence of racial hatred or racial vilification
11	An offence relating to firearms, ammunition, weapons or the use of an item as a weapon
12	An offence relating to explosives or explosive devices
13	Arson or an offence of a kind equivalent to arson
14	An offence relating to production, possession, supply, import or export of an illegal drug or controlled substance
15	An offence relating to illegal import or export of goods, fauna or flora
16	An offence relating to interference with goods under customs control
17	An offence relating to extortion or blackmail
18	An offence relating to theft (other than offences referred to in clauses 1and 2 of this Schedule)
19	An offence relating to forgery or fraud
20	An offence relating to tax evasion
21	An offence relating to money laundering or currency violations
22	An offence relating to dealing with proceeds of crime

Replaced Authorised Version registered 19/04/2024 F2021C00921

Maritime-security-relevant offences—tier 3 offences	
Item	**Offence**
23	An offence relating to bribery or corruption
24	An offence of perjury or otherwise relating to perversion of the course of justice
25	An offence relating to use of a false identity or false identity documents
26	An offence relating to the unauthorised use, access, modification or destruction of data or electronic communications

Note: A person convicted of an offence mentioned in the table and sentenced to imprisonment will have an adverse criminal record (see the definition of ***adverse criminal record*** in subregulation 6.07B(3)).

Replaced Authorised Version registered 19/04/2024 F2021C00921

Schedule 2—Transitional arrangements

(regulation 14.01)

Part 1—Amendments made by Maritime Transport and Offshore Facilities Security Amendment Regulation 2012 (No. 3)

101 Operation of Schedule 1

The amendments of these Regulations made by Schedule 1 to the *Maritime Transport and Offshore Facilities Security Amendment Regulation 2012 (No. 3)* (the ***amending regulation***) do not apply to:

(a) an application under section 50 of the Act by a port facility operator or a port service provider for an approval of a maritime security plan made, but not determined, before the commencement of the amending regulation; or

(b) an application under section 52A of the Act by a port facility operator or a port service provider for a variation of a maritime security plan made, but not determined, before the commencement of the amending regulation; or

(c) for a maritime security plan approved before the commencement of the amending regulation—an application under section 52A of the Act by a port facility operator or a port service provider for a variation of the maritime security plan made after the commencement of the amending regulation.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 2—Amendments made by the Customs and Other Legislation Amendment (Australian Border Force) Regulation 2015

102 Things done by the Australian Customs and Border Protection Service

(1) A thing done by, or in relation to, the Australian Customs and Border Protection Service under these Regulations before 1 July 2015 has effect on and after that day as if it had been done by, or in relation to, the Comptroller-General of Customs.

(2) Without limiting subclause (1), if the Australian Customs and Border Protection Service was an issuing body under Division 6.1A of Part 6 of these Regulations immediately before 1 July 2015, then, on and after that day, the Comptroller-General of Customs is taken to be an issuing body under that Division.

(3) Without limiting subclause (1), if an MSIC plan was in force in relation to the Australian Customs and Border Protection Service immediately before 1 July 2015, then, on and after that day, the plan is taken to be in force in relation to the Immigration and Border Protection Department.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 3—Amendments made by the Transport Security Legislation Amendment (Job Ready Status) Regulation 2015

103 Applications for MSICs

The amendments of these Regulations made by Part 2 of Schedule 1 to the *Transport Security Legislation Amendment (Job Ready Status) Regulation 2015* apply in relation to an application for an MSIC made on or after the commencement of that Part.

Note: Part 2 of Schedule 1 to the *Transport Security Legislation Amendment (Job Ready Status) Regulation 2015* commenced on 15 December 2015.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 4—Amendments made by the Transport Security Legislation Amendment (Identity Security) Regulation 2016

104 Amendments made by the *Transport Security Legislation Amendment (Identity Security) Regulation 2016* and commencing 1 November 2016

MSIC plans

(1) Despite the repeal and substitution of regulation 6.07Q of the old regulations by item 19 of Schedule 2 to the amending regulation, an issuing body's MSIC plan that is in effect under Division 6.1A of Part 6 of the old regulations immediately before 1 November 2016 has effect, during the issuing body's implementation period, as if it were a plan of the kind described in regulation 6.07Q of the new regulations.

(2) However, subclause (1) does not:
  (a) prevent the Secretary giving a direction to an issuing body under regulation 6.07S, or revoking an issuing body's authorisation under regulation 6.07W because of the issuing body's MSIC plan, on or after 1 November 2016; or
  (b) affect a direction given by the Secretary to an issuing body under regulation 6.07S before 1 November 2016 and not complied with before that day.

(3) If subclause (1) applies to an issuing body's MSIC plan, the issuing body must give the Secretary the document required by subregulation 6.07Q(4) of the new regulations on 1 November 2016, or as soon as practicable afterwards.

(4) If:
  (a) subclause (1) applies to an issuing body's MSIC plan; and
  (b) before the end of 1 December 2016, the issuing body submits to the Secretary a proposed variation of the issuing body's MSIC plan under paragraph 6.07T(1)(b) for the purposes of complying with the new regulations;

regulation 6.07T applies in relation to the proposed variation as if each reference to 30 days in subregulation 6.07T(3) were a reference to 60 days.

Requirement to retain records and documents

(5) The amendment made by item 71 of Schedule 2 to the amending regulation applies in relation to:
  (a) an application for an MSIC made to an issuing body on or after 1 November 2016; and
  (b) an MSIC issued as a result of such an application.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Person directly involved in the issue of MSICs

(6) Subject to subclause (7), the amendments made by items 23, 24, 29, 30 and 31 of Schedule 2 to the amending regulation apply to an issuing body on and after 1 November 2016.

(7) The amendments made by items 23, 24, 29, 30 and 31 of Schedule 2 to the amending regulation apply, in relation to a person who was directly involved in the issue of MSICs at any time within the period of 2 years ending on 1 November 2016, at the earlier of the following times (but not before 1 November 2016):

(a) the end of 2 years after the person's most recent background check applied for under regulation 6.08BA of the old regulations was completed;

(b) the start of 1 August 2017.

Definitions

(8) In this clause:

amending regulation means the *Transport Security Legislation Amendment (Identity Security) Regulation 2016*.

implementation period, in relation to an issuing body, means the period that begins on 1 November 2016 and ends:

(a) if, before the end of 1 December 2016, the issuing body submits to the Secretary a proposed variation of the issuing body's MSIC plan under paragraph 6.07T(1)(b) for the purposes of complying with the new regulations—at the end of the earlier of the following days:

(i) the day the Secretary approves the variation in accordance with regulation 6.07T;

(ii) 1 February 2017; or

(b) otherwise—at the end of 1 December 2016.

new regulations means these Regulations as in force on and after 1 November 2016.

Note: 1 November 2016 is the day Part 1 of Schedule 2 to the amending regulation commences.

old regulations means these Regulations as in force immediately before 1 November 2016.

105 Amendments made by the *Transport Security Legislation Amendment (Identity Security) Regulation 2016* and commencing 1 August 2017

The amendments made by Part 2 of Schedule 2 to the *Transport Security Legislation Amendment (Identity Security) Regulation 2016* apply in relation to applications for MSICs made on or after 1 August 2017.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 5—Amendments made by the Transport Security Legislation Amendment (Security Assessments) Regulation 2016

106 Amendments made by the *Transport Security Legislation Amendment (Security Assessments) Regulation 2016*

The amendments made by Schedule 2 to the *Transport Security Legislation Amendment (Security Assessments) Regulation 2016* apply in relation to:

(a) an application for an MSIC made to an issuing body on or after 1 November 2016; and

(b) an MSIC issued as a result of such an application.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 6—Amendments made by the Transport Security Legislation Amendment (Issuing Body Processes) Regulation 2016

107 Amendments made by the *Transport Security Legislation Amendment (Issuing Body Processes) Regulation 2016*

(1) Subject to subclause (2), the amendments of these Regulations made by Schedule 2 to the *Transport Security Legislation Amendment (Issuing Body Processes) Regulation 2016* apply in relation to the following:

(a) a decision of the Secretary made on or after 1 November 2016 to revoke the authorisation of a body as an issuing body (including such a decision made on the basis of matters that arose before that day);

(b) any other event referred to in subregulation 6.07ZA(1) that occurs on or after 1 November 2016.

(2) The amendments of these Regulations made by Schedule 2 to the *Transport Security Legislation Amendment (Issuing Body Processes) Regulation 2016* apply in relation to an application for the Secretary to revoke the authorisation of a body as an issuing body made on or after 1 November 2016.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 7—Amendments made by the Transport Security Legislation Amendment (ASIC and MSIC Measures) Regulations 2018

108 Amendments made by the *Transport Security Legislation Amendment (ASIC and MSIC Measures) Regulations 2018*

(1) Despite the amendments of these Regulations by Schedule 2 to the amending regulations, an MSIC that was:

(a) issued under the old regulations; and

(b) in force immediately before the commencement time;

continues to be valid and in force (and subject to the same conditions) on and after the commencement time until the end of the period for which it was issued under the old regulations, unless it is suspended or cancelled in accordance with these Regulations before the end of that period.

(2) Despite the amendments of regulation 6.08J of these Regulations by Schedule 2 to the amending regulations, regulation 6.08J of these Regulations has effect for an issuing body during the body's transition period as if it required an MSIC to be, and authorised the body to issue an MSIC, in the form set out in regulation 6.08J of the old regulations.

(3) In this clause:

amending regulations means the *Transport Security Legislation Amendment (ASIC and MSIC Measures) Regulations 2018*.

commencement time means the time when this clause commences.

old regulations means these Regulations as in force immediately before the commencement time.

transition period, for an issuing body, means the period starting at the commencement time and ending at the earlier of the following times:

(a) at the end of 3 months starting at the commencement time;

(b) at the time the Secretary first gives the issuing body an approved form under regulation 6.08JA.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 8—Amendments made by the Transport Security Legislation Amendment (2019 Measures No. 1) Regulations 2019

109 Training and qualifications requirements for maritime security guards

Regulation 8.50, as substituted by Schedule 1 to the *Transport Security Legislation Amendment (2019 Measures No. 1) Regulations 2019*, applies in relation to training and qualifications requirements for maritime security guards on and after the day that is 12 months after the day that Schedule commenced.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 9—Amendments made by the AusCheck Legislation Amendment (2019 Measures No. 1) Regulations 2019

110 Applications for additional background checks

For the purposes of paragraph 6.08BA(b), as inserted by the *AusCheck Legislation Amendment (2019 Measures No. 1) Regulations 2019*, it does not matter whether the previous application was made before, on or after 1 July 2019.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 10—Amendments made by the Transport Security Legislation Amendment (Foreign Officials) Regulations 2021

111 Amendments made by the *Transport Security Legislation Amendment (Foreign Officials) Regulations 2021*

The amendments of these Regulations made by Schedule 1 to the *Transport Security Legislation Amendment (Foreign Officials) Regulations 2021* do not apply in relation to an MSIC in force immediately before the commencement of that Schedule.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Part 11—Amendments made by the Transport Security Legislation (Serious Crime) Regulations 2021

112 Definitions

In this Part:

amended Regulations means these Regulations as amended by the amending Regulations.

amending Regulations means the *Transport Security Legislation (Serious Crime) Regulations 2021*.

convicted has the same meaning as in Division 6.1A of the amended Regulations.

old Regulations means these Regulations as in force immediately before the commencement of the amending Regulations.

113 Continued application of old Regulations

Despite the amendments made to these Regulations by the amending Regulations, the old Regulations continue to apply in relation to the following:

(a) an application for a background check made before the commencement of the amending Regulations;

(b) an application made to the Secretary under regulation 6.08F that:

(i) is made before the commencement of the amending Regulations; or

(ii) relates to the outcome of a background check to which the old Regulations apply;

(c) an application made to the Secretary under regulation 6.08MA before the commencement of the amending Regulations.

114 Obligation to report past conviction for maritime-security-relevant offence

(1) This regulation applies in relation to a person who is the holder of, or an applicant for, an MSIC when the amending Regulations commence if:

(a) before that commencement, the person was:

(i) convicted of and sentenced for a tier 1 offence or a tier 2 offence (within the meaning of Division 6.1A of the amended Regulations); or

(ii) convicted of, and sentenced to imprisonment for, a tier 3 offence (within the meaning of Division 6.1A of the amended Regulations); and

(b) the offence was not a maritime-security-relevant offence within the meaning of Division 6.1A of the old Regulations.

Replaced Authorised Version registered 19/04/2024 F2021C00921

(2) The person must notify the issuing body for the MSIC or the Secretary, in writing, of the matters in paragraphs 6.08LB(2)(a) to (e) in relation to the offence within 30 days after the day the amending Regulations commence.

(3) A person commits an offence if:
  (a) the person is required to notify an issuing body or the Secretary under subregulation (2) in relation to an offence; and
  (b) the person fails to comply with the requirement.

  Penalty: 20 penalty units.

(4) The following provisions of the amended Regulations apply in relation to notification under subregulation (2) of this regulation as if it were notification under subregulation 6.08LB(2) of the amended Regulations:
  (a) paragraph 6.08BA(c);
  (b) subregulations 6.08LB(3) to (5);
  (c) regulation 6.08LBA;
  (d) paragraph 6.08M(1)(h).

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnotes

Endnote 1—About the endnotes

The endnotes provide information about this compilation and the compiled law.

The following endnotes are included in every compilation:

Endnote 1—About the endnotes
Endnote 2—Abbreviation key
Endnote 3—Legislation history
Endnote 4—Amendment history

Abbreviation key—Endnote 2
The abbreviation key sets out abbreviations that may be used in the endnotes.

Legislation history and amendment history—Endnotes 3 and 4
Amending laws are annotated in the legislation history and amendment history.

The legislation history in endnote 3 provides information about each law that has amended (or will amend) the compiled law. The information includes commencement details for amending laws and details of any application, saving or transitional provisions that are not included in this compilation.

The amendment history in endnote 4 provides information about amendments at the provision (generally section or equivalent) level. It also includes information about any provision of the compiled law that has been repealed in accordance with a provision of the law.

Editorial changes
The *Legislation Act 2003* authorises First Parliamentary Counsel to make editorial and presentational changes to a compiled law in preparing a compilation of the law for registration. The changes must not change the effect of the law. Editorial changes take effect from the compilation registration date.

If the compilation includes editorial changes, the endnotes include a brief outline of the changes in general terms. Full details of any changes can be obtained from the Office of Parliamentary Counsel.

Misdescribed amendments
A misdescribed amendment is an amendment that does not accurately describe the amendment to be made. If, despite the misdescription, the amendment can be given effect as intended, the amendment is incorporated into the compiled law and the abbreviation “(md)” added to the details of the amendment included in the amendment history.

If a misdescribed amendment cannot be given effect as intended, the abbreviation “(md not incorp)” is added to the details of the amendment included in the amendment history.

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 2—Abbreviation key

ad = added or inserted

am = amended

amdt = amendment

c = clause(s)

C[x] = Compilation No. x

Ch = Chapter(s)

def = definition(s)

Dict = Dictionary

disallowed = disallowed by Parliament

Div = Division(s)

ed = editorial change

exp = expires/expired or ceases/ceased to have effect

F = Federal Register of Legislation

gaz = gazette

LA = *Legislation Act 2003*

LIA = *Legislative Instruments Act 2003*

(md) = misdescribed amendment can be given effect

(md not incorp) = misdescribed amendment cannot be given effect

mod = modified/modification

No. = Number(s)

o = order(s)

Ord = Ordinance

orig = original

par = paragraph(s)/subparagraph(s) /sub-subparagraph(s)

pres = present

prev = previous

(prev…) = previously

Pt = Part(s)

r = regulation(s)/rule(s)

reloc = relocated

renum = renumbered

rep = repealed

rs = repealed and substituted

s = section(s)/subsection(s)

Sch = Schedule(s)

Sdiv = Subdivision(s)

SLI = Select Legislative Instrument

SR = Statutory Rules

Sub-Ch = Sub-Chapter(s)

SubPt = Subpart(s)

underlining = whole or part not commenced or to be commenced

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 3—Legislation history

Number and year	FRLI registration or gazettal	Commencement	Application, saving and transitional provisions
366, 2003	23 Dec 2003	Part 1, Part 3 (except Subdivision 3.4.1), Part 4, rr. 6.05, 6.20, 6.80, 6.85, 6.105, Part 12 and Part 13: 1 Jan 2004 Remainder: 1 July 2004 (r. 1.02(b) and gaz 2004, No GN11)	
34, 2004	18 Mar 2004	rr. 1–3 and Schedule 1: 18 Mar 2004 Remainder: 1 July 2004 (r. 2(b) and gaz 2004, No GN11)	—
137, 2004	18 June 2004	rr. 1–4 and Schedule 1: 18 June 2004 Remainder: 1 July 2004 (r. 2(b) and gaz 2004, No GN11)	—
195, 2004	1 July 2004	rr. 1–4 and Schedule 1: 1 July 2004 Remainder: 1 July 2004 (r. 2(b) and gaz 2004, No GN11)	—
115, 2005	8 June 2005 (F2005L01407)	9 June 2005	—
158, 2005	8 July 2005 (F2005L01919)	9 July 2005	—
201, 2005	2 Sept 2005 (F2005L02436)	rr. 1–3 and Schedule 1: 3 Sept 2005 Remainder: 30 Sept 2005 (r. 2(b))	—
209, 2005	16 Sept 2005 (F2005L02675)	17 Sept 2005	—
225, 2005	7 Oct 2005 (F2005L03031)	8 Oct 2005	—
186, 2006	14 July 2006 (F2006L02347)	15 July 2006	—
202, 2006	28 July 2006 (F2006L02475)	29 July 2006	—
372, 2006	15 Dec 2006 (F2006L04099)	1 Jan 2007	—
42, 2007	23 Mar 2007 (F2007L00726)	27 Mar 2007 (r. 2)	—
173, 2007	26 June 2007 (F2007L01803)	rr. 1–3 and Schedule 1: 1 July 2007 Remainder: 3 Sept 2007	—
11, 2009	6 Feb 2009 (F2009L00256)	7 Feb 2009	—
291, 2009	9 Nov 2009 (F2009L04049)	10 Nov 2009	—
178, 2010	30 June 2010 (F2010L01818)	rr. 1–3, 5 and Schedule 1: 1 July 2010 r. 4 and Schedule 2: 1 Dec 2010	r. 5

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 3—Legislation history

Number and year	FRLI registration or gazettal	Commencement	Application, saving and transitional provisions
299, 2010	26 Nov 2010 (F2010L03068)	1 Dec 2010 (r 2)	—
140, 2011	3 Aug 2011 (F2011L01595)	r 4 and Sch 2: 11 Sept 2011 (r 2(b)) Remainder: 4 Aug 2011 (r 2(a))	—
136, 2012	29 June 2012 (F2012L01421)	1 July 2012 (s 2)	—
214, 2012	3 Sept 2012 (F2012L01824)	4 Sept 2012 (s 2)	—
258, 2012	27 Nov 2012 (F2012L02263)	Sch 2: 1 Feb 2013 (s 2(b)) Remainder: 28 Nov 2012 (s 2(a))	—
120, 2013	18 June 2013 (F2013L01031)	19 June 2013 (s 2)	—
49, 2015	21 Apr 2015 (F2015L00580)	22 Apr 2015 (s 2)	—
90, 2015	19 June 2015 (F2015L00854)	Sch 2 (items 127–131): 1 July 2015 (s 2(1) item 2)	—
174, 2015	2 Nov 2015 (F2015L01739)	30 June 2016 (s 2(1) item 1)	—
248, 2015	14 Dec 2015 (F2015L01966)	Sch 1 (items 19–36): 15 Dec 2015 (s 2(1) item 1)	—

Name	Registration	Commencement	Application, saving and transitional provisions
Biosecurity (Consequential Amendments and Transitional Provisions) Regulation 2016	9 May 2016 (F2016L00717)	Sch 2 (items 21–24) and Sch 3: 16 June 2016 (s 2(1) item 1)	Sch 3
Maritime Transport and Offshore Facilities Security Amendment (Inter-State Voyages) Regulation 2016	19 Aug 2016 (F2016L01309)	20 Aug 2016 (s 2(1) item 1)	—
Transport Security Legislation Amendment (Identity Security) Regulation 2016	28 Oct 2016 (F2016L01656)	Sch 2 (items 1–77): 1 Nov 2016 (s 2(1) item 4) Sch 2 (items 78–88): 1 Aug 2017 (s 2(1) item 5)	—
Transport Security Legislation Amendment (Security Assessments) Regulation 2016	28 Oct 2016 (F2016L01659)	Sch 2: 1 Nov 2016 (s 2(1) item 3)	—
Transport Security Legislation Amendment (Issuing Body Processes) Regulation 2016	28 Oct 2016 (F2016L01660)	Sch 2: 1 Nov 2016 (s 2(1) item 3)	—
AusCheck and Other Laws (Repeal and Consequential Amendments) Regulations 2017	31 July 2017 (F2017L00972)	Sch 1 (items 6–8): 1 Aug 2017 (s 2(1) item 1)	—

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 3—Legislation history

Name	Registration	Commencement	Application, saving and transitional provisions
Transport Security Legislation Amendment (ASIC and MSIC Measures) Regulations 2018	26 Nov 2018 (F2018L01603)	Sch 2: 27 Nov 2018 (s 2(1) item 1)	—
AusCheck Legislation Amendment (Required Information) Regulations 2019	22 Mar 2019 (F2019L00355)	Sch 1 (item 30): 1 July 2019 (s 2(1) item 1)	—
Transport Security Legislation Amendment (2019 Measures No. 1) Regulations 2019	17 June 2019 (F2019L00829)	Sch 1 (items 65–91): 18 June 2019 (s 2(1) item 1)	—
AusCheck Legislation Amendment (2019 Measures No. 1) Regulations 2019	19 June 2019 (F2019L00840)	Sch 2 (items 4, 5): 1 July 2019 (s 2(1) item 5)	—
Crimes Legislation Amendment (2019 Measures No. 1) Regulations 2019	26 July 2019 (F2019L01004)	Sch 1 (item 3): 27 July 2019 (s 2(1) item 1)	—
Transport Security Legislation Amendment (Repeal of Screening Officer Requirements) Regulations 2021	1 June 2021 (F2021L00675)	Sch 1 (item 3): 15 June 2021 (s 2(1) item 1)	—
Maritime Transport and Offshore Facilities Security Amendment (Security Awareness Training) Regulations 2021	1 June 2021 (F2021L00677)	1 July 2021 (s 2(1) item 1)	—
Transport Security Legislation Amendment (Foreign Officials) Regulations 2021	9 July 2021 (F2021L00971)	Sch 1 (items 8–10): 10 July 2021 (s 2(1) item 1)	—
Transport Security Legislation Amendment (Serious Crime) Regulations 2021	20 Aug 2021 (F2021L01145)	Sch 1 (items 38–68): 23 Aug 2021 (s 2(1) item 1)	—

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
Part 1	
r. 1.01	am. 2005 No. 158
r 1.02	am 2005 No 209
	rep LA s 48D
r 1.03	am No 34, 2004; No 137, 2004; No 158, 2005; No 201, 2005; No 11, 2009; No 140, 2011; No 174, 2015; F2016L01309; F2016L01656; F2016L01659; F2019L00829
r. 1.04	am. 2005 No. 158
r. 1.05	rs. 2004 No. 34
	am No 174, 2015
r. 1.06	ad. 2005 No. 158
r 1.10	am No 174, 2015
r. 1.15	am No 11, 2009; No 174, 2015
r 1.20	am No 174, 2015; F2021L00677
r 1.25	am No 174, 2015; F2021L00677
r 1.30	rep No 174, 2015
r. 1.32	ad. 2005 No. 158
r. 1.33	ad. 2005 No. 158
r. 1.34	ad. 2005 No. 158
r. 1.35	am No 158, 2005; No 174, 2015
r. 1.45	am No 158, 2005; No 201, 2005; No 11, 2009; No 174, 2015
r 1.50	am No 158, 2005; F2019L00829
r 1.55	am No 34, 2004; No 137, 2004; No 158, 2005; No 140, 2011; F2019L00829
r. 1.56	ad. 2004 No. 34
	am. 2005 No. 158; 2011 No. 140
r. 1.65	am. 2005 No. 158
r 1.72	ad F2016L01309
r 1.75	ad 2004 No 34
	am F2016L01309
r. 1.80	ad. 2004 No. 34
r 1.85	ad 2011 No 140
	rep F2016L01309
Part 2	
Division 2.2	
Division 2.2	rs. 2004 No. 34
	am. 2004 No. 34
r 2.25	ad No 34, 2004
	am F2019L00829

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
Division 2.3	
r. 2.30	am. 2005 Nos. 158 and 201
r 2.35	rs No 34, 2004
	am No 158, 2005; No 201, 2005; F2019L00829
Part 3	
Division 3.1	
r 3.10	am No 174, 2015; F2019L00829
r. 3.11	ad No. 258, 2012
r. 3.12	ad No 201, 2005
	rep No 291, 2009
	ad No 258, 2012
	am No 174, 2015
r 3.15	am No 174, 2015
r 3.20	am No 174, 2015
r 3.25	rep No 174, 2015
Division 3.2	
Subdivision 3.2.1 heading	rep. 2012 No. 258
r. 3.35	am. 2004 No. 34; 2006 No. 372
r. 3.77	ad. 2004 No. 137
Subdivision 3.2.2	rep. 2012 No. 258
r. 3.90	rs. 2011 No. 140
	rep. 2012 No. 258
r. 3.95	rep. 2012 No. 258
Division 3.3	
Subdivision 3.3.1 heading	rep. 2012 No. 258
r. 3.100	am No 372, 2006
r 3.105	rs No 174, 2015
r. 3.106	ad. 2004 No. 34
r 3.130	am No 174, 2015
r. 3.155	rs. 2011 No. 140
r 3.160	am 2004 No 137; F2016L01309
Subdivision 3.3.2	rep. 2012 No. 258
r. 3.165	rep. 2012 No. 258
r. 3.170	rep. 2012 No. 258
Division 3.4	rep No 174, 2015
r 3.175	rep No 174, 2015
r 3.180	rep No 174, 2015
r. 3.185	am No 372, 2006
	rep No 174, 2015
r 3.190	rep No 174, 2015

Replaced Authorised Version registered 19/04/2024 F2021C00921

Provision affected	How affected
r. 3.191	ad. 2004 No. 34
	rep No 174, 2015
r 3.195	rep No 174, 2015
r 3.200	rep No 174, 2015
r 3.205	rep No 174, 2015
r. 3.210	am. 2004 No. 34
	rep No 174, 2015
r 3.215	rep No 174, 2015
r 3.220	rep No 174, 2015
r 3.225	rep No 174, 2015
r 3.230	rep No 174, 2015
r 3.235	rep No 174, 2015
Subdivision 3.4.3	rep No 258, 2012
r. 3.240	rep No 258, 2012
r. 3.245	rep No 258, 2012
Part 4	
Division 4.2	
r. 4.20	am. 2004 No. 34; 2011 No. 140
r. 4.30	am. 2006 No. 372
r. 4.31	ad. 2004 No. 34
r. 4.45	am No 34, 2004; No 158, 2005; No 174, 2015
r. 4.65	am. 2004 No. 137
r. 4.80	am. 2004 Nos. 34 and 195; 2011 No. 140
r 4.85	rs No 158, 2005; No 201, 2005
	am F2019L00829
r 4.90	am F2019L00829
r. 4.95	am. 2011 No. 140
r. 4.100	am. 2004 No. 34
r 4.105	am F2019L00829
r. 4.110	am. 2011 No. 140
Division 4.4	
Division 4.4	ad. 2004 No. 34
	rs. 2011 No. 140
	am. 2004 No. 34
	rs. 2011 No. 140
r 4.120	ad No 140, 2011
	am F2019L00829
r. 4.125	ad. 2011 No. 140
Division 4.5	
Division 4.5	ad. 2004 No. 34

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
r. 4.140	ad. 2004 No. 34
	am. 2011 No. 140
r. 4.145	ad. 2004 No. 34
r 4.150	ad No 140, 2011
	am F2019L00829
r. 4.155	ad. 2011 No. 140
Part 5	
Division 5.1	
Division 5.1	rs. 2004 No. 34
r. 5.10	ad. 2004 No. 34
	am. 2004 No. 195
Division 5.2	
r 5.25	rs No 34, 2004
	am F2019L00829
Part 5A	
Part 5A	ad. 2005 No. 158
Division 5A.1	
r. 5A.05	ad. 2005 No. 158
r 5A.10	ad No 158, 2005
	am No 201, 2005; F2019L00829
r. 5A.12	ad. 2005 No. 201
	rep. 2009 No. 291
r. 5A.15	ad. 2005 No. 158
	rep. 2005 No. 201
	ad. 2005 No. 201
r. 5A.20	ad. 2005 No. 158
Division 5A.2	
Subdivision 5A.2.1	
r. 5A.25	ad. 2005 No. 158
r. 5A.30	ad. 2005 No. 158
	am. 2006 No. 372
r. 5A.35	ad. 2005 No. 158
r. 5A.40	ad. 2005 No. 158
r. 5A.45	ad. 2005 No. 158
r. 5A.50	ad. 2005 No. 158
r. 5A.55	ad. 2005 No. 158
r 5A.60	ad No 158, 2005
	am No 11, 2009; F2019L00829
r. 5A.65	ad. 2005 No. 158
r. 5A.70	ad. 2005 No. 158

Replaced Authorised Version registered 19/04/2024 F2021C00921

Provision affected	How affected
r. 5A.75	ad. 2005 No. 158
r. 5A.80	ad. 2005 No. 158
r. 5A.85	ad. 2005 No. 158
	am. 2005 No. 201
r. 5A.90	ad. 2005 No. 158
r. 5A.92	ad. 2009 No. 11
Subdivision 5A.2.2	
r. 5A.95	ad. 2005 No. 158
r. 5A.100	ad. 2005 No. 158
r. 5A.105	ad. 2005 No. 158
Division 5A.3	
Subdivision 5A.3.1	
r. 5A.110	ad. 2005 No. 158
Subdivision 5A.3.2	
r. 5A.115	ad. 2005 No. 158
r. 5A.120	ad. 2005 No. 158
	am. 2006 No. 372
r. 5A.125	ad. 2005 No. 158
r. 5A.130	ad. 2005 No. 158
r. 5A.135	ad. 2005 No. 158
r. 5A.140	ad. 2005 No. 158
r. 5A.145	ad. 2005 No. 158
r. 5A.150	ad. 2005 No. 158
r. 5A.155	ad. 2005 No. 158
r. 5A.160	ad. 2005 No. 158
r. 5A.165	ad. 2005 No. 158
r. 5A.170	ad. 2005 No. 158
r. 5A.175	ad. 2005 No. 158
Part 6	
Division 6.1	
r 6.05	am 2004 No 137; No 90, 2015
Division 6.1A	
Division 6.1A	ad. 2005 No. 201
Subdivision 6.1A.1	
r. 6.07A	ad. 2005 No. 201
	am. 2006 No. 202; 2006 No. 372; 2009 No. 291; 2010 No. 178; F2016L01656
r 6.07B	ad No 201, 2005
	am No 202, 2006; No 372, 2006; No 173, 2007; No 291, 2009; No 178, 2010; No 299, 2010; F2016L01656; F2016L01660; F2017L00972; F2018L01603; F2019L00829; F2019L01004; F2021L00971; F2021L01145

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
r. 6.07C	ad. 2005 No. 201
	am No 291, 2009
	rep. 2010 No. 178
r. 6.07D	ad. 2005 No. 201
	rs. 2006 No. 372
	am. 2010 No. 178; F2016L01656
r. 6.07E	ad. 2005 No. 201
	rs. 2006 No. 372
	am F2016L01656
r. 6.07F	ad 2005 No 201
	am No 248, 2015; F2016L01656; F2021L00971
r 6.07G	ad No 201, 2005
	am No 372, 2006
	rep F2016L01656
r 6.07H	ad No 201, 2005
r 6.07HA	ad No 202, 2006
	rep No 291, 2009
	ad F2016L01656
Subdivision 6.1A.1A	ad No 202, 2006
	rep No 291, 2009
r 6.07HB	ad No 202, 2006
	rep No 291, 2009
r 6.07HC	ad No 202, 2006
	rep No 291, 2009
r 6.07HD	ad No 202, 2006
	rep No 291, 2009
r 6.07HE	ad No 202, 2006
	rep No 291, 2009
Subdivision 6.1A.2	
r. 6.07I	ad. 2005 No. 201
	am. 2006 No. 372
r. 6.07J	ad. 2005 No. 201
	am. 2006 No. 372; No 49, 2015; F2016L01656
r 6.07K	ad 2005 No 201
	am 2007 No 173; F2021L01145
r. 6.07L	ad. 2005 No. 201
r. 6.07M	ad. 2005 No. 201
	am. 2006 No. 372; F2016L01656
r. 6.07N	ad. 2005 No. 201
	am. 2006 No. 372

Replaced Authorised Version registered 19/04/2024 F2021C00921

Provision affected	How affected
Subdivision 6.1A.3	
Subdivision 6.A1.3 heading.....	rep. 2006 No. 202
Subdivision 6.1A.3 heading.....	ad. 2006 No. 202
r 6.07O.....	ad No 201, 2005
	am No 90, 2015
r. 6.07P.....	ad. 2005 No. 201
	am. 2010 No. 178; F2016L01656
r. 6.07Q.....	ad. 2005 No. 201
	rs F2016L01656
r. 6.07R.....	ad. 2005 No. 201
	am. 2010 No. 178; F2016L01656
r. 6.07S.....	ad. 2005 No. 201
	am F2016L01656
r. 6.07T.....	ad. 2005 No. 201
	am. 2010 No. 178; F2016L01656
r. 6.07U.....	ad. 2005 No. 201
r. 6.07V.....	ad. 2005 No. 201
	am F2016L01656
r. 6.07W.....	ad. 2005 No. 201
	am. 2010 No. 178; F2016L01656
	rs F2016L01660
r. 6.07X.....	ad. 2005 No. 201
	rs F2016L01660
r. 6.07Y.....	ad. 2005 No. 201
	rs F2016L01660
r. 6.07Z.....	ad. 2005 No. 201
	rs F2016L01660
r 6.07ZA.....	ad F2016L01660
r 6.07ZB.....	ad F2016L01660
Subdivision 6.1A.4	
Subdivision 6.1A.4 heading.....	rs. 2010 No. 178
r 6.08A.....	ad 2005 No 201
	am 2010 No 178
	rep F2021L01145
r. 6.08B.....	ad No 201, 2005
	am No 372, 2006; No 173, 2007
	rs No 173, 2007; No 178, 2010
	am No 136, 2012; No 248, 2015; F2016L01656
r 6.08BA.....	ad No 173, 2007

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
	am No 178, 2010; No 299, 2010; No 248, 2015; F2016L01656; F2019L00840; F2021L01145
r 6.08BB	ad F2016L01656
	am F2017L00972
	ed C34
r 6.08BC	ad F2016L01656
r 6.08C	ad No 201, 2005
	am No 372, 2006; No 173, 2007; No 299, 2010; No 136, 2012; F2016L01656; F2016L01659; F2019L00829
r. 6.08CA	ad. 2007 No. 173
	rep. 2009 No. 291
	ad. 2010 No. 299
	am. 2012 No. 136; F2016L01656
r 6.08D	ad 2005 No 201
	am 2006 No 372; 2007 No 173; F2021L01145
r. 6.08E	ad. 2005 No. 201
	am F2016L01656
r 6.08F	ad No 201, 2005
	am No 372, 2006; No 173, 2007; No 178, 2010; No 136, 2012; No 248, 2015; F2016L01656; F2021L01145
r 6.08G	ad No 201, 2005
	rep No 372, 2006
r 6.08H	ad 2005 No 201
	am 2007 No 173
	rs 2007 No 173
	am 2010 No 178; F2021L01145
r. 6.08HA	ad. 2007 No. 173
	am. 2010 No. 178
r. 6.08I	ad. 2005 No. 201
	am. 2007 No. 173; 2010 Nos. 178 and 299; 2012 No. 136; F2016L01656; F2016L01659; F2018L01603
r 6.08J	ad No 201, 2005
	am No 186, 2006; No 372, 2006; No 299, 2010; F2016L01656; F2018L01603
r 6.08JA	ad F2018L01603
r 6.08JB	ad F2018L01603
r. 6.08K	ad. 2005 No. 201
	rs. 2006 No. 372
	am. 2007 No. 173; 2009 No. 291; F2016L01656
r. 6.08KA	ad. 2006 No. 372
	am F2016L01656
r. 6.08L	ad. 2005 No. 201

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
	am. 2006 No. 372; 2007 No. 173
	rs F2016L01656
	am F2018L01603
r. 6.08LA	ad. 2007 No. 173
	am F2016L01656
r 6.08LB	ad No 178, 2010
	rs No 299, 2010
	am No 248, 2015; F2021L01145
r. 6.08LBA	ad No 299, 2010
	rs No 214, 2012
	am No 248, 2015
r 6.08LC	ad No 178, 2010
	am No. 299, 2010; No 248, 2015; F2021L01145
r 6.08LCA	ad F2016L01656
	am F2016L01656
r 6.08LD	ad No 178, 2010
	am No 299, 2010
	rs No 214, 2012
	am F2016L01656
	ed C33
r. 6.08LDA	ad No 214, 2012
	am F2016L01656
r 6.08LE	ad No 178, 2010
	am F2016L01656; F2021L01145
r. 6.08LF	ad No 178, 2010
	am F2016L01656
r 6.08LG	ad No 178, 2010
	rs F2021L01145
r. 6.08LH	ad No 178, 2010
r. 6.08LI	ad No 178, 2010
	am No 299, 2010
r 6.08M	ad No 201, 2005
	am No 372, 2006; No 178, 2010; No 299, 2010; No 140, 2011; No 136, 2012; No 214, 2012; F2016L01656; F2017L00972; F2019L00355; F2021L01145
	ed C42
r 6.08MA	ad 2010 No 178
	am F2021L01145
r. 6.08MB	ad. 2010 No. 178
	am. 2010 No. 299
r 6.08MC	ad No 178, 2010

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
	am No 299, 2010; F2021L01145
r. 6.08MD	ad. 2010 No. 178
r. 6.08N	ad. 2005 No. 201
	am F2016L01656
r 6.08O	ad 2005 No 201
	rs 2006 No 372
	am F2021L01145
r. 6.08P	ad. 2005 No. 201
	am F2016L01656
r. 6.08Q	ad. 2005 No. 201
	am F2016L01656
r. 6.08R	ad. 2005 No. 201
	am F2016L01656
Subdivision 6.1A.5	
Subdivision 6.1A.5 heading	rs. 2006 No. 372
r. 6.08S	ad. 2005 No. 201
	am. 2006 No. 372; 2009 No. 291; F2016L01656
Subdivision 6.1A.6	
r. 6.08T	ad. 2005 No. 201
	am. 2010 No. 178
r. 6.08U	ad. 2005 No. 201
	am F2016L01656
r. 6.08V	ad. 2005 No. 201
	am. 2010 No. 178; F2016L01656
Subdivision 6.1A.7	
r. 6.08W	ad. 2005 No. 201
r 6.08X	ad No 201, 2005
	am No 372, 2006; No 178, 2010; F2016L01656; F2016L01660
r. 6.08Y	ad. 2005 No. 201
	am F2016L01656
r. 6.08Z	ad. 2005 No. 201
Subdivision 6.1A.8	
r. 6.09A	ad. 2005 No. 201
	rs. 2006 No. 372
Division 6.2	
Subdivision 6.2.2	
r. 6.33	ad. 2004 No. 137
r. 6.40	am No 137, 2004; No 11, 2009
	rep No 174, 2015
r. 6.45	am No 137, 2004; No 174, 2015

Replaced Authorised Version registered 19/04/2024 F2021C00921

Provision affected	How affected
Subdivision 6.2.3	
r. 6.50	am. 2011 No. 140
Subdivision 6.2.4	
r. 6.65	rs. 2004 No. 34
	am. 2004 No. 137
r. 6.70	rs. 2005 No. 115
Division 6.3	
r. 6.85	am. 2009 No. 11
r. 6.90	am. 2005 No. 115; 2009 No. 11
r. 6.95	rs. 2005 No. 115
	am. 2009 No. 11
r. 6.96	ad. 2009 No. 11
r. 6.100	rs. 2009 No. 11
Division 6.5	
Division 6.5	ad. 2005 No. 158
	rep. 2005 No. 201
	ad. 2005 No. 201
r. 6.150	am. 2009 No. 11
Subdivision 6.5.1	
Subdivision 6.5.1 heading	ad. 2005 No. 201
r. 6.125	ad. 2005 No. 158
	rep. 2005 No. 201
	ad. 2005 No. 201
Subdivision 6.5.2	
Subdivision 6.5.2 heading	ad. 2005 No. 201
r. 6.130	ad. 2005 No. 158
	rep. 2005 No. 201
	ad. 2005 No. 201
r. 6.135	ad. 2005 No. 158
	rep. 2005 No. 201
	ad. 2005 No. 201
r. 6.140	ad. 2005 No. 158
	rep. 2005 No. 201
	ad. 2005 No. 201
Subdivision 6.5.3	
Subdivision 6.5.3 heading	ad. 2005 No. 201
r. 6.145	ad. 2005 No. 158
	rep. 2005 No. 201
	ad. 2005 No. 201
r. 6.150	ad. 2005 No. 158

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
	rep. 2005 No. 201
	ad. 2005 No. 201
r. 6.155	ad. 2005 No. 158
	rep. 2005 No. 201
	ad. 2005 No. 201
Part 7	
Division 7.1	
r 7.05	rs No 137, 2004
	am No 90, 2015
Division 7.2	
r 7.20	am 2004 No 137; F2016L01309
r 7.25	am 2004 No 137; 2005 No 115; F2016L00717; F2016L01309
r 7.27	ad 2004 No 137
	am F2016L01309
r 7.28	ad 2004 No 137
	am F2016L01309
r 7.29	ad 2004 No 137
	am F2016L01309
r 7.30	rs 2010 No 178
	am F2016L01309
r 7.31	ad 2010 No 178
r 7.33	ad 2004 No 34
r 7.34	ad 2012 No 258
r 7.35	am 2004 No 137; F2016L01309
Division 7.3	
Division 7.3	rs. 2005 No. 115
r 7.39	ad No 115, 2005
	am F2019L00829
r. 7.40	am. 2004 Nos. 34 and 137
	rs. 2005 No. 115
	am F2016L00717
r. 7.45	rs. 2005 No. 115
	am F2016L00717
r. 7.50	am. 2004 No. 34
	rs. 2005 No. 115
	am F2016L00717
r. 7.55	ad. 2005 No. 115
Part 8	
Division 8.2	
Division 8.2	rs. 2004 No. 34

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
r. 8.20A	ad. 2005 No. 115
r. 8.20	ad. 2004 No. 34
Division 8.2A	
Division 8.2A	ad. No. 120, 2013
r. 8.25	ad. No. 120, 2013
Division 8.4	
r 8.40	am No 90, 2015
Division 8.5	
Division 8.5	ad. 2004 No. 34
Subdivision 8.5.1	
Subdivision 8.5.1 heading	ad. 2007 No. 42
r 8.50	ad No 34, 2004
	rs F2019L00829
r. 8.55	ad. 2004 No. 34
	am. 2007 No. 42
Subdivision 8.5.2	
r. 8.57	ad. 2007 No. 42
r. 8.58	ad. 2007 No. 42
Division 8.6	ad 2004 No 34
	rep F2021L00675
r 8.60	ad 2004 No 34
	rep F2021L00675
r 8.65	ad 2004 No 34
	rep F2021L00675
Part 9	
Part 9	rs. 2005 Nos. 158 and 201
Part 11	
Part 11	rs. 2005 No. 225
Division 11.2	
Division 11.2	ad. 2005 No. 225
r. 11.05	ad. 2005 No. 225
r. 11.10	ad. 2005 No. 225
r. 11.15	ad. 2005 No. 225
r. 11.20	ad. 2005 No. 225
r. 11.25	ad. 2005 No. 225
r. 11.30	ad. 2005 No. 225
r. 11.35	ad. 2005 No. 225
r. 11.40	ad. 2005 No. 225
r. 11.45	ad. 2005 No. 225
r. 11.50	ad. 2005 No. 225

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 4—Amendment history

Provision affected	How affected
r. 11.55	ad. 2005 No. 225
r. 11.60	ad. 2005 No. 225
r. 11.65	ad. 2005 No. 225
r 11.70	ad No 225, 2005
	am F2019L00829
r. 11.75	ad. 2005 No. 225
r. 11.80	ad. 2005 No. 225
Division 11.6	
Division 11.6	ad. 2005 No. 225
r. 11.300	ad. 2005 No. 225
r. 11.305	ad. 2005 No. 225
r. 11.310	ad. 2005 No. 225
r. 11.315	ad. 2005 No. 225
r. 11.320	ad. 2005 No. 225
r. 11.325	ad. 2005 No. 225
r. 11.330	ad. 2005 No. 225
r. 11.335	ad. 2005 No. 225
Part 12	
Part 12	rs. 2009 No. 11
r. 12.01	ad. 2009 No. 11
Part 13	
r. 13.05	am. 2004 No. 34; 2011 No. 140
Part 14	
Part 14	ad. 2012 No. 258
r. 14.01	ad. 2012 No. 258
Schedule 1	
Schedule 1	ad 2010 No 178
	rs F2021L01145
Schedule 2	
Schedule 2	ad No 258, 2012
Part 1	
c 101	ad No 258, 2012
Part 2	
Part 2	ad No 90, 2015
c 102	ad No 90, 2015
Part 3	
Part 3	ad No 248, 2015
c 103	ad No 248, 2015
Part 4	
Part 4	ad F2016L01656

Replaced Authorised Version registered 19/04/2024 F2021C00921

Provision affected	How affected
c 104	ad F2016L01656
c 105	ad F2016L01656
Part 5	
Part 5	ad F2016L01659
c 106	ad F2016L01659
Part 6	
Part 6	ad F2016L01660
c 107	ad F2016L01660
Part 7	
Part 7	ad F2018L01603
c 108	ad F2018L01603
	ed C37
Part 8	
Part 8	ad F2019L00829
c 109	ad F2019L00829
Part 9	
Part 9	ad F2019L00840
c 110	ad F2019L00840
Part 10	
Part 10	ad F2021L00971
c 111	ad F2021L00971
Part 11	
Part 11	ad F2021L01145
c 112	ad F2021L01145
c 113	ad F2021L01145
c 114	ad F2021L01145

Replaced Authorised Version registered 19/04/2024 F2021C00921

Endnote 5—Editorial changes

In preparing this compilation for registration, the following kinds of editorial change(s) were made under the *Legislation Act 2003*.

Paragraph 6.08M(1)(e)

Kind of editorial change

Removal of redundant text

Details of editorial change

Schedule 1 item 59 of the *Transport Security Legislation Amendment (Serious Crime) Regulations 2021* instructs to repeal and substitute paragraphs 6.08M(1)(e) and (ea).

The newly inserted paragraph 6.08M(1)(e) reads in part "the issuing body has a received a notice from the Secretary".

This compilation was editorially changed to omit "a received a" and substitute "received a" to remove the redundant text.

Replaced Authorised Version registered 19/04/2024 F2021C00921