Reprint
as at 1 April 2021

Maritime Security Regulations 2004

(SR 2004/153)

Silvia Cartwright, Governor-General

Order in Council

At Wellington this 31st day of May 2004

Present:
Her Excellency the Governor-General in Council

Pursuant to section 76 of the Maritime Security Act 2004, Her Excellency the Governor-General, acting on the advice and with the consent of the Executive Council, makes the following regulations.

Contents

Note

Changes authorised by subpart 2 of Part 2 of the Legislation Act 2012 have been made in this official reprint.

Note 4 at the end of this reprint provides a list of the amendments incorporated.

These regulations are administered by the Ministry of Transport.

Regulations

1 Title

These regulations are the Maritime Security Regulations 2004.

2 Commencement

(1) Regulations 5 to 22, 31 and 32, 43 and 44, and 58 to 62 come into force on 1 July 2004.

(2) The rest of these regulations come into force on the day after the date of their notification in the *Gazette*.

3 Interpretation

In these regulations, unless the context otherwise requires, **Act** means the Maritime Security Act 2004.

4 Persons responsible for complying with requirements imposed on ships

(1) The master of a ship is responsible for complying with a requirement imposed by these regulations that applies in relation to the ship.

(2) If the ship is a New Zealand ship, the company is responsible for ensuring the master of the ship complies with the requirement.

Part 1
Declaration of security

5 Declaration of security to be acknowledged

(1) The master or ship security officer must acknowledge every requirement of, or request made by, any of the following persons for the ship to complete a declaration of security:

(a) the chief executive:

(b) the master or ship security officer of another ship:

(c) a port facility security officer.

(2) The port facility security officer must acknowledge every requirement of, or request made by, any of the following persons for the port facility to complete a declaration of security:

(a) the chief executive:

(b) the master or ship security officer of a ship.

Compare: Code, Part A s 5.3

6 Persons who must complete declaration of security

(1) A declaration of security completed on behalf of a ship must be completed by—

(a) the master; or

(b) the ship security officer; or

(c) a senior ship officer authorised by the master.

(2) A declaration of security completed on behalf of a port facility must be completed by—

(a) the port facility security officer; or

(b) any other person designated by the port facility operator as responsible for the security of that port facility.

Compare: Code, Part A s 5.4

7 Declaration of security to specify responsibility for security requirements

A declaration of security must specify—

(a) the security requirements for which a ship and a port facility, or a ship and another ship, as the case may require, are separately responsible; and

(b) the security requirements that are to be shared between—

(i) a ship and a port facility; or

(ii) a ship and another ship; and

(c) the specific responsibilities (if any) that a ship and a port facility, or a ship and another ship, as the case may require, have in relation to the security requirements that are to be shared; and

(d) the duration of the declaration of security.

Compare: Code, Part A s 5.5, Part B s 5.4.1

8 Minimum period for ships to keep declaration of security

Every New Zealand ship that has completed a declaration of security must keep the declaration of security for the next 10 calls at a port facility.

Compare: Code, Part A s 5.7

9 Minimum period for port facilities to keep declaration of security

(1) Every port facility that completes a declaration of security must keep the declaration of security for a period of 12 months after the date on which the duration of the declaration of security has ended.

(2) A copy of all current declarations of security must be kept with the port facility security plan.

Compare: Code, Part A s 5.6

Part 2
Ship security

Threats to ships

10 Threats to ships

If a risk of attack to a ship has been identified, the chief executive must advise the master of the ship and the ship's administration of—

(a) the current security level; and

(b) any security measures that may, in accordance with the Act and these regulations, be put in place by the ship concerned to protect itself from attack; and

(c) security measures that the chief executive has decided to put in place as appropriate.

Compare: Annex to the Convention, Chapter XI-2 r 7.3

11 Reporting of security threats and security breaches

(1) A company must, without delay, report to the New Zealand Police any act or circumstance that may threaten a ship's security.

(2) As soon as possible after complying with subclause (1), the company must make a report in writing, giving a summary of the activity or breach,—

(a) to the Designated Authority; and

(b) if the report relates to cargo or ship stores, to the New Zealand Customs Service.

Ship security levels

12 Commencement level

Unless otherwise directed by the chief executive, every New Zealand ship must operate at security level 1 from 1 July 2004 unless otherwise directed by—

(a) the chief executive; or

(b) a state that is a party to the Convention if that ship is in a port within that state.

13 Chief executive to advise ship of certain matters when specifying security level for ship

When specifying the security level for a ship, the chief executive must advise the ship of—

(a) any security measures that it should take; and

(b) if appropriate, any security measures that have been taken by the Designated Authority to provide protection against any potential maritime security threat.

Compare: Code, Part A s 7.9.1

14 Security level 1

(1) At security level 1, a ship must carry out through appropriate measures the following activities to identify and take preventive measures against security incidents:

(a) ensure the performance of all ship security duties:

(b) control access to the ship:

(c) control the embarkation of persons and their effects:

(d) monitor restricted areas to ensure that only authorised personnel have access:

(e) monitor deck areas and areas surrounding the ship:

(f) supervise the handling of cargo and ship stores:

(g) ensure that security communication is readily available.

(2) At security level 1, a ship must implement the security measures and procedures for security level 1 as specified in its approved ship security plan.

Compare: Code, Part A s 7.2

15 Security level 2

At security level 2, a ship must implement the additional protective measures and procedures specified in its approved ship security plan for each activity specified in regulation 14.

Compare: Code, Part A s 7.3

16 Security level 3

At security level 3, a ship must respond to and implement any further specific protective measures and procedures specified in its approved ship security plan for each activity specified in regulation 14.

Compare: Code, Part A s 7.4

17 Specification for security level 2 or security level 3 to be acknowledged

A ship whose security level is specified as, or is changed to, security level 2 or security level 3 by the chief executive must—

(a) provide acknowledgment to the Designated Authority of the security level specification; and

(b) respond, without undue delay, to the security level specification.

Compare: Annex to the Convention, Chapter XI-2 r 4.4; Code, Part A s 7.5

18 Additional responsibilities for ship with security level 2 or security level 3

(1) Before entering a port, or while in a port, a ship whose security level specification is security level 2 or security level 3 must—

(a) start implementing the appropriate measures and procedures specified in the approved ship security plan (including, in the case of a ship with a security level 3 specification, the further protective measures specified by the chief executive); and

(b) inform the port facility security officer that it has started to implement the appropriate measures and procedures referred to in paragraph (a).

(2) If a ship has any difficulties in implementing the appropriate measures and procedures referred to in subclause (1)(a), the master of the ship or a ship security officer must report, as soon as practicable, those difficulties to the port facility security officer.

(3) If the master of a ship or a ship security officer reports difficulties in implementing the appropriate measures and procedures referred to in subclause (1)(a) to the port facility security officer, the ship security officer and the port facility security officer must liaise about, and co-ordinate the appropriate response to, those difficulties.

Compare: Code, Part A s 7.6

19 Requirements for non-complying ships

(1) Before conducting any ship-port interface or entering a port (whichever occurs first), a ship that is unable to comply with the Act or these regulations, or to meet the requirements set for its security level by the chief executive or by a State that is a party to the Convention, must notify the port facility security officer of that fact.

(2) If a ship has any difficulties in implementing the appropriate measures and procedures for its security level, the ship must report those difficulties to the port facility security officer.

(3) If a ship reports difficulties in implementing the appropriate measures and procedures for its security level to the port facility security officer, the ship security officer and the port facility security officer must liaise about, and co-ordinate the appropriate response to, those difficulties.

Compare: Annex to the Convention, Chapter XI-2 r 4.5; Code, Part A s 7.6

20 Notification of ship with security level 2 or security level 3 in port facility outside New Zealand

If the chief executive specifies the security level of a New Zealand ship in a port facility of a State that is a party to the Convention as security level 2 or security level 3, the chief executive must, without undue delay, notify the government of the State of that port facility accordingly.

Compare: Code, Part A s 7.8

21 Requirements for ship with higher security level than port facility

(1) A ship whose security level specification is higher than the level specified for the port facility that it is about to enter or has already entered, must, without undue delay, advise the Designated Authority and the port facility security officer of the situation.

(2) If a situation described in subclause (1) occurs, the ship security officer and the port facility security officer must liaise about, and co-ordinate the response to, the situation.

Compare: Code, Part A ss 7.7, 7.7.1

22 Chief executive to advise ships to report certain information

When the chief executive specifies a security level and provides security level information to a ship that is either operating within the territorial limits of New Zealand or has communicated to the chief executive its intention to enter the territorial limits of New Zealand, the chief executive must advise the master of the ship to report immediately to all the following persons any information that comes to the master's attention that might affect maritime security in the area:

(a) the chief executive:

(b) the ship's Administration.

Compare: Code, Part A s 7.9

Ship security assessment

23 Ship security assessment

(1) A ship security assessment must include (but is not limited to) the following:

(a) include an on-scene survey:

(b) identify and evaluate key shipboard operations that require protection:

(c) identify possible threats to those key shipboard operations and the likelihood of their occurrence in order to establish and prioritise security measures:

(d) identify existing security measures, procedures, and operations:

(e) identify weaknesses, including human factors, in the infrastructure, policies, and procedures:

(f) address the following elements on board or within the ship:

(i) physical security:

(ii) structural integrity:

(iii) personnel protection systems:

(iv) procedural policies:

(v) radio and telecommunication systems, including computer systems and networks:

(vi) other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility.

(2) A ship security assessment must consider all possible threats, including the following types of security incidents:

(a) damage to or destruction of the ship or an interfacing port facility or ship by dangerous substances and devices, arson, sabotage, or vandalism:

(b) hijacking or seizure of the ship or of persons on board:

(c) tampering with cargo, essential ship equipment or systems, or ship stores:

(d) unauthorised access to, or use of, the ship, cargo, essential ship equipment or systems, or ship stores:

(e) smuggling dangerous substances and ship devices:

(f) use of the ship to carry persons intending to cause a security incident:

(g) use of a ship to carry equipment intended to cause a security incident:

(h) use of the ship or its equipment as a weapon or as a means to cause damage or destruction:

(i) attacks from seaward while at berth or at anchor:

(j) attacks while at sea:

(k) presence of stowaways.

(3) A ship security assessment must consider the persons, activities, services, and operations that are important to protect, including (but not limited to)—

(a) ship personnel and port facility personnel:

(b) passengers, visitors, vendors, repair technicians, and other persons working on ships or in port facilities:

(c) the capacity to maintain safe navigation and emergency response:

(d) the cargo, particularly dangerous goods or hazardous substances:

(e) ship stores:

(f) the ship security communications equipment and systems (if any):

(g) the ship's security surveillance equipment and systems (if any).

(4) A ship security assessment must consider the continuing relevance of existing security measures and guidance, procedures and operations, under both routine and emergency conditions.

(5) A ship security assessment must take into account all possible vulnerabilities, including (but not limited to)—

(a) conflicts between safety and security measures:

(b) conflicts between shipboard duties and security assignments:

(c) watchkeeping duties, number of ship personnel, particularly with implications for crew fatigue, alertness, and performance:

(d) any identified security training deficiencies:

(e) any security equipment and systems, including communications systems.

(6) The company must document, review, accept, and retain the ship security assessment.

Compare: Code, Part A ss 8.4, 8.5, Part B, ss 8.3, 8.8–8.10

24 Ship security assessment may be kept in electronic form

A ship security assessment may be kept in electronic form, in which case the company must ensure that it is protected from unauthorised deletion, destruction, amendment, disclosure, or access.

Compare: Code, Part B s 4.1

25 Requirements of person conducting ship security assessment

The company must ensure that the person who carries out the ship security assessment has appropriate knowledge of the following matters:

(a) current security threats and patterns:

(b) the recognition and detection of weapons, dangerous substances, and devices:

(c) the recognition on a non-discriminatory basis of characteristics and behavioural patterns of persons who are likely to threaten security:

(d) the techniques used to circumvent security measures:

(e) the methods used to cause a security incident:

(f) the effects of explosives on ship structures and equipment:

(g) ship security:

(h) ship-port interface business practices:

(i) contingency planning, emergency preparedness, and response:

(j) physical security:

(k) radio and telecommunications systems, including computer systems and networks:

(l) marine engineering:

(m) ship and port operations.

Compare: Code, Part B s 8.4

26 On-scene surveys of ships

The on-scene survey must examine and evaluate existing ship protective measures, procedures, and operations for—

(a) ensuring the performance of all security duties:

(b) monitoring restricted areas to ensure that access is only granted to persons with appropriate authority:

(c) controlling access to the ship, through the use of identification systems or otherwise:

(d) monitoring of deck areas and areas surrounding the ship:

(e) controlling the embarkation of persons and their effects (including accompanied and unaccompanied baggage and ship personnel personal effects):

(f) supervising the handling of cargo and the delivery of ship stores:

(g) ensuring that ship security communications, information systems, and equipment are readily available.

Compare: Code, Part B s 8.14

Restricted areas

27 Restricted areas

(1) The ship security plan must identify the restricted areas to be established on the ship, and specify—

(a) their extent; and

(b) the times of application; and

(c) the security measures to be taken to control access to them; and

(d) the security measures to be taken to control activities within them.

(2) The purposes of restricted areas are to—

(a) prevent unauthorised access; and

(b) protect passengers, ship personnel, and personnel from port facilities or other agencies authorised to be on board the ship; and

(c) protect security-sensitive areas within the ship; and

(d) protect cargo and ship stores from being tampered with.

(3) Restricted areas may include, as appropriate,—

(a) the navigation bridge, machinery spaces of category A, and other control stations as defined in Chapter II-2 of the Annex to the Convention:

(b) spaces containing security and surveillance equipment and systems and their controls, and lighting system controls:

(c) ventilation and air-conditioning systems and other similar spaces:

(d) spaces with access to tanks, pumps, or manifolds for potable water:

(e) spaces containing dangerous goods or hazardous substances:

(f) spaces containing cargo pumps and their controls:

(g) cargo spaces and spaces containing ship stores:

(h) crew accommodation:

(i) any other areas as determined by the company security officer, through the ship security assessment, to which access must be restricted to maintain the security of the ship.

Compare: Code, Part B ss 9.18, 9.21

28 Security measures for restricted areas at security level 1

At security level 1, the ship security plan must establish the security measures that apply to restricted areas, which may include—

(a) locking of security access points:

(b) using surveillance equipment to monitor the areas:

(c) using guards or patrols:

(d) using automatic intrusion-detection devices to alert the ship personnel of unauthorised access.

Compare: Code, Part B s 9.22

29 Security measures for restricted areas at security level 2

At security level 2,—

(a) the frequency and intensity of the monitoring of, and control of access to, restricted areas must be increased to ensure that only authorised persons have access; and

(b) the ship security plan must establish the additional security measures that apply, which may include—

(i) establishing restricted areas adjacent to access points:

(ii) continuously monitoring surveillance equipment:

(iii) dedicating additional personnel to guard and patrol restricted areas.

Compare: Code, Part B s 9.23

30 Security measures for restricted areas at security level 3

At security level 3,—

(a) the ship must comply with the instructions issued by those responding to the security incident or threat; and

(b) the ship security plan must detail the security measures that could be taken by the ship, in close co-operation with those responding and the port facility, which may include—

(i) setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied:

(ii) searching of restricted areas as part of a search of the ship.

Compare: Code, Part B s 9.24

Advice required of ships intending to enter ports

31 Appropriate ship security procedures

When a master provides advice under section 30(2)(e) of the Act concerning whether or not appropriate ship security procedures were maintained in any ship-to-ship activity during the period of its last 10 calls at port, the master—

(a) must include in that advice the following matters (if applicable):

(i) the measures taken while engaged in a ship-to-ship activity with a ship that is registered in a State that is not a party to the Convention:

(ii) the measures taken while engaged in a ship-to-ship activity with a ship that is registered in a State that is a party to the Convention but that is not required to comply with any of the provisions of the Act or these regulations, or Chapter XI-2 of the Annex to the Convention and Part A of the Code:

(iii) any persons or goods rescued at sea and that are on board, including all known information about the persons or goods; but

(b) need not include in that advice the following matters if they are already covered by the port facility security plan:

(i) transfers of pilots:

(ii) transfers of customs, immigration, or security officials:

(iii) bunkering:

(iv) lightering:

(v) loading of supplies:

(vi) unloading of waste by the ship within port facilities.

Compare: Code, Part B s 4.38

32 Other practical security-related matters

When a master provides advice under section 30(2)(f) of the Act concerning any other practical security-related matters, the master must include in that advice the following matters (if applicable):

(a) information contained in the continuous synopsis record:

(b) location of the ship at the time the report is made:

(c) expected time of arrival of the ship in port:

(d) crew list:

(e) general description of cargo aboard the ship:

(f) passenger list:

(g) information required to be carried under the Annex to the Convention, Chapter XI-2 regulation 5.

Compare: Code, Part B s 4.39

Ship security plan

33 Ship security plan approval

A company must submit—

(a) 1 copy of the ship security plan to the chief executive for review and approval; and

(b) a letter certifying that the ship security plan complies with the Act and these regulations.

34 Chief executive to give notice where ship security plan covers more than 1 ship

If the chief executive agrees that a ship security plan may cover more than 1 ship, he or she must give notice of the arrangement to the International Maritime Organization.

35 Language used for ship security plan

(1) A ship security plan must be written in the working language of the ship.

(2) Despite subclause (1), if the working language of the ship is not English, French, or Spanish, a written translation of the ship security plan into 1 of those languages must be included with the ship security plan.

Compare: Code, Part A s 9.4

36 Matters to be included in ship security plan

(1) Without limiting the matters that a ship security plan may contain, a ship security plan must include the matters specified in Schedule 1.

(2) Despite subclause (1), the chief executive may authorise the company to keep the information on the ship's security alert system, set out in clauses (m) and (n) of Schedule 1, in a separate document in a location on the ship known only to the master, the ship security officer, and any other senior shipboard personnel that the company may designate for that purpose.

Compare: Code, Part A s 9.4

37 Confidential matters in ship security plan not to be disclosed

The matters referred to in clauses (c), (e), (h), (i)(i), (j), (m), (n), and (o) of Schedule 1 are confidential, and, except as provided in section 32(3) and (4) of the Act, may not be inspected by the chief executive.

Compare: Code, Part A s 9.8

38 Security assessment to accompany ship security plan

The following must, when submitted to the chief executive for approval, be accompanied by the security assessment that is the basis for the plan or amendments:

(a) a ship security plan; and

(b) any amendments to a previously approved ship security plan.

Compare: Code, Part A s 9.3

39 Ship security plan may be kept in electronic form

A ship security plan may be kept in electronic form, in which case the company must ensure that it is protected from unauthorised deletion, destruction, or amendment.

Compare: Code, Part A s 9.6

40 Ship security plan to be audited

(1) The company must ensure an audit of the ship security plan is performed annually, beginning no later than 1 year from the initial date of approval.

(2) The ship security plan must be audited if there is a change in the ship's ownership or operator, or if there have been modifications to the ship, including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) An audit of the ship security plan as a result of modifications to the ship may be limited to those sections of the ship security plan affected by the vessel modifications.

Compare: Code, Part B s 9.53

41 Audits of ship security plan to be independent

(1) Company or ship personnel who conduct internal audits of the security activities specified in the ship security plan or who evaluate the implementation of the ship security plan must be independent of the activities being audited.

(2) Subclause (1) does not apply if this is impracticable because of the size and the nature of the company or the ship.

Compare: Code, Part A s 9.4.1

Recognised security organisations

42 Competencies of recognised security organisations

Before the chief executive may authorise an organisation to be a recognised security organisation under section 9(1)(j) of the Act, the chief executive must ensure that the organisation—

(a) has appropriate expertise in relevant aspects of security; and

(b) has appropriate knowledge of ship and port operations, including knowledge of ship design and construction if providing services in respect of ships and port design, and construction if providing services in respect of port facilities; and

(c) is competent to assess the likely security risks that could occur during ship and port facility operations, including the ship-port interface and how to minimise those risks; and

(d) is competent to maintain and improve the expertise of the organisation's personnel; and

(e) is competent to monitor the continuing trustworthiness of the organisation's personnel; and

(f) is competent to maintain appropriate measures to avoid unauthorised disclosure of, or access to, security-sensitive material; and

(g) has appropriate knowledge of the Convention and the Code as well as the relevant requirements of New Zealand law and international law; and

(h) has appropriate knowledge of current security threats and patterns; and

(i) is competent to recognise and detect weapons, dangerous substances, and dangerous devices; and

(j) is competent to recognise characteristics and behavioural patterns of persons who are likely to threaten security; and

(k) has appropriate knowledge of techniques used to circumvent security measures; and

(l) has appropriate knowledge of security and surveillance equipment and systems and their operational limitations.

Compare: Code, Part B s 4.5

Ship security alert system

43 Ships to have ship security alert system

(1) A ship constructed on or after 1 July 2004 must have a ship security alert system.

(2) A passenger ship, including high-speed passenger craft, constructed before 1 July 2004 must have a ship security alert system not later than the first survey of the radio installation after 1 July 2004.

(3) An oil tanker, chemical tanker, gas carrier, bulk carrier, or cargo high-speed craft, of 500 gross tonnage or more, constructed before 1 July 2004 must have a ship security alert system not later than the first survey of the radio installation after 1 July 2004.

(4) Cargo ships of 500 gross tonnage or more, other than those specified in subclause (3) or mobile offshore drilling units, constructed before 1 July 2004 must have a ship security alert system not later than the first survey of the radio installation after 1 July 2006.

Compare: Annex to the Convention, Chapter XI-2 r 6.1

44 Requirements for ship security alert system

(1) A ship security alert system must—

(a) be capable of being activated from the navigation bridge and at least 1 other location; and

(b) conform to performance standards that are not inferior to those adopted by the International Maritime Organization.

(2) A ship security alert system of a New Zealand ship, when activated, must initiate and transmit a ship-to-shore alert to a competent authority designated by the chief executive, which may include the company, that—

(a) identifies the ship and its location; and

(b) indicates that the security of the ship is under threat or is compromised; and

(c) continues the alert until deactivated or reset.

(3) A ship security alert system, when activated, must not—

(a) send the alert to any other ship; or

(b) raise any alarm on board the ship sending the alert.

(4) The activation points of the ship security alert system must be designed so as to prevent the inadvertent initiation of the alert.

(5) The requirement for a ship security alert system may be met by using the radio installation fitted in compliance with Chapter IV of the Annex to the Convention as long as all the requirements of this regulation are met.

Compare: Annex to the Convention, Chapter XI-2 rr 6.2–6.5

Company security officer

45 Company security officer

(1) A person may be designated as the company security officer for 1 or more ships if all the ships for which the company security officer is responsible are clearly identified.

(2) A company may designate more than 1 person as company security officer for a ship if the ship for which each company security officer is responsible is clearly identified in the designation.

Compare: Code, Part A s 11.1

46 Duties and responsibilities of company security officer

The duties and responsibilities of a company security officer in relation to each ship for which he or she is responsible include—

(a) advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information; and

(b) ensuring that ship security assessments are carried out; and

(c) ensuring the development, the submission for approval and, after its approval, the implementation and maintenance of the ship security plan; and

(d) ensuring that the ship security plan is modified, as appropriate, to correct deficiencies in the plan and satisfy the security requirements of the ship; and

(e) arranging for internal audits and reviews of security activities; and

(f) arranging for the initial and subsequent verifications of the ship by the chief executive; and

(g) ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections, and verifications of compliance are promptly addressed and dealt with; and

(h) enhancing security awareness and vigilance; and

(i) ensuring adequate training for personnel responsible for the security of the ship; and

(j) ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officer; and

(k) ensuring consistency between security requirements and safety requirements; and

(l) ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and

(m) ensuring that any alternative or equivalent arrangements approved for a ship or class of ships are implemented and maintained.

Compare: Code, Part A s 11.2

Ship security officer

47 Ship security officer

(1) The company must designate a ship security officer on each ship.

(2) The duties and responsibilities of the ship security officer include—

(a) undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained; and

(b) maintaining and supervising the implementation of the ship security plan, including any amendments to the plan; and

(c) co-ordinating the security aspects of the handling of cargo and ship stores with other shipboard personnel, the relevant port facility security officer, and the New Zealand Customs Service; and

(d) proposing modifications to the ship security plan; and

(e) reporting to the company security officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections, and verifications of compliance, and implementing any corrective actions; and

(f) enhancing security awareness and vigilance on board; and

(g) ensuring that adequate training has been provided to shipboard personnel, as appropriate; and

(h) reporting all security incidents; and

(i) co-ordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and

(j) ensuring that all security equipment is properly operated, tested, calibrated, and maintained.

Compare: Code, Part A s 12

Training, drills, and exercises on ship security

48 Company security officer, ship security officer, and shore-based personnel to have adequate knowledge and training

(1) The company must ensure that the company security officer, the ship security officer and appropriate shore-based personnel have an adequate knowledge of, and relevant training in the following ship security procedures (if applicable):

(a) security administration:

(b) the relevant international conventions, codes, and recommendations:

(c) the relevant New Zealand and international legislation:

(d) the responsibilities and functions of relevant security organisations:

(e) the methodology of ship security assessment:

(f) the methods of ship security surveys and inspections:

(g) ship and port operations and conditions:

(h) ship and port facility security measures:

(i) emergency preparedness and response and contingency planning:

(j) the instruction techniques for security training and education, including security measures and procedures:

(k) the handling of sensitive security-related information and security-related communications:

(l) current security threats and patterns:

(m) the recognition and detection of weapons, dangerous substances, and dangerous devices:

(n) the recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of people who are likely to threaten security:

(o) the techniques used to circumvent security measures:

(p) security equipment and systems and their operational limitations:

(q) the methods of conducting audits, inspection, control, and monitoring:

(r) the methods of searches and non-intrusive inspections:

(s) security drills and exercises, including drills and exercises with port facilities:

(t) the assessment of security drills and exercises.

(2) The company must ensure that the ship security officer has adequate knowledge of, and training in the following matters:

(a) the layout of the ship:

(b) the ship security plan and related procedures (including scenario-based training on how to respond):

(c) crowd management and control techniques:

(d) operations of security equipment and systems:

(e) testing, calibrating, and, while at sea, maintaining security equipment and systems.

(3) The company must ensure that—

(a) the company security officer has completed the standard International Maritime Organization course for company security officers; and

(b) the ship security officer has completed the standard International Maritime Organization course for ship security officers.

Compare: Code, Part A ss 13.1, 13.2, Part B ss 13.1, 13.2

49 Shipboard personnel to have adequate knowledge and training

(1) The company must ensure that shipboard personnel who have specific security duties and responsibilities—

(a) understand their responsibilities for ship security as described in the ship security plan; and

(b) have an adequate knowledge of, and ability to perform, their assigned security duties, including the following if they are applicable:

(i) current security threats and patterns:

(ii) the recognition and detection of weapons, dangerous substances, and dangerous devices:

(iii) the recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of people who are likely to threaten security:

(iv) the techniques used to circumvent security measures:

(v) crowd management and control techniques:

(vi) security-related communications:

(vii) emergency procedures and contingency plans:

(viii) the operation of security equipment and systems:

(ix) testing, calibrating, and, while at sea, maintaining security equipment and systems:

(x) inspection, control, and monitoring techniques:

(xi) the methods of searches and non-intrusive inspections.

(2) The company must ensure that all shipboard personnel who are not covered by subclause (1) have an adequate knowledge of, and are familiar with, the relevant provisions of the ship security plans, including—

(a) the meaning and requirements of security level 1, security level 2, and security level 3; and

(b) emergency procedures and contingency plans; and

(c) the recognition and detection of weapons, dangerous substances, and dangerous devices; and

(d) the recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of people who are likely to threaten security; and

(e) the techniques used to circumvent security measures.

Compare: Code, Part A s 13.3, Part B ss 13.3, 13.4

50 Company to carry out drills

(1) Taking into account the ship type, ship personnel changes, port facilities to be visited, and other relevant factors, the company must ensure the effective implementation of the ship security plan by carrying out drills at least every 3 months.

(2) If, as a result of a change in shipboard personnel, more than 25% of the shipboard personnel have not participated within the previous 3 months in an exercise or drill on that ship, a drill must be conducted within 1 week of the change in shipboard personnel.

(3) The drills referred to in subclause (2) must test the separate elements of the ship security plan and cover all possible threats to the security of the ship, including, but not limited to, the following types of security incidents:

(a) damage to or destruction of the ship or an interfacing port facility or ship by dangerous substances and devices, arson, sabotage, or vandalism:

(b) hijacking or seizure of the ship or of persons on board:

(c) tampering with cargo, essential ship equipment or systems, or ship stores:

(d) unauthorised access to, or use of, the ship, cargo, essential ship equipment or systems, or ship stores:

(e) smuggling dangerous substances and ship devices:

(f) use of the ship to carry persons intending to cause a security incident:

(g) use of a ship to carry equipment intended to cause a security incident:

(h) use of the ship or its equipment as a weapon or as a means to cause damage or destruction:

(i) attacks from seaward while at berth or at anchor:

(j) attacks while at sea:

(k) presence of stowaways.

Compare: Code, Part A s 13.4, Part B ss 8.9, 13.6

51 Company to facilitate exercises

(1) A company must, at least once every calender year (with no more than 18 months between the exercises), facilitate the holding of exercises that test communication, co-ordination, resource availability, and response.

(2) The exercises may involve—

(a) representatives of the Designated Authority; and

(b) representatives of the chief executives of the organisations listed in section 59(1)(a)(ii) of the Act; and

(c) the company security officer; and

(d) depending on the security and work implications for the New Zealand ships to which the Act applies, the ship security officer; and

(e) depending on the security and work implications for the port facility, the port facility security officer.

(3) The exercises may be—

(a) full scale or live, or both; or

(b) tabletop simulations or seminars, or both; or

(c) combined with other exercises held, such as emergency response or other exercises involving state and port authorities.

(4) The chief executive may direct that the requirements of subclauses (1) to (3) may alternatively be satisfied by—

(a) participation of company staff in an emergency response or crisis management exercise conducted by another government agency or private sector entity, provided that the exercise addresses components of the ship security plan; or

(b) an actual increase in security level; or

(c) implementation of enhanced security measures enumerated in the ship security plan during periods of critical port operations or special events; or

(d) participation of company staff in an exercise with another contracting government.

Compare: Code, Part B ss 13.7, 13.8

52 Company security officer to participate in exercises and drills

The company security officer must, taking into account the guidance given in Part B of the Code, ensure the effective co-ordination and implementation of

ship security plans by participating in drills and exercises under regulations 50 and 51 at appropriate intervals.

Compare: Code, Part A s 13.5

Ship security records

53 Ship security records

(1) The master and the company must ensure that records of the following matters included in the ship security plan (ship security records) are kept on board the ship that cover, at least, the last 10 calls at a port facility:

(a) training, drills, and exercises:

(b) security threats and security incidents:

(c) breaches of security:

(d) changes in security level:

(e) communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been, in:

(f) internal audits and reviews of security activities:

(g) periodic review of the ship security assessment:

(h) periodic review of the ship security plan:

(i) implementation of any amendments to the plan:

(j) maintenance, calibration, and testing of any security equipment provided on board, including testing of the ship security alert system.

(2) A master of a ship and its company must ensure that the ship has available on board, at all times, information through which a person authorised by the chief executive or officers duly authorised by the Designated Authorities of other parties to the Convention may establish—

(a) who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship; and

(b) who is responsible for deciding the employment of the ship; and

(c) if the ship is employed under terms of a charter party, who are the parties to that charter party.

Compare: Annex to the Convention, Chapter XI-2 r 5; Code, Part A s 10.1

54 Language used for ship security records

(1) All ship security records must be written in the working language of the ship.

(2) Despite subclause (1), if the working language of the ship is not English, French, or Spanish, a written translation of the ship security records into 1 of those languages must be included with the ship security records.

Compare: Code, Part A s 10.2

55 Ship security records may be kept in electronic form

Ship security records may be kept in electronic form, in which case they must be protected from unauthorised deletion, destruction, or amendment.

Compare: Code, Part A s 10.3

56 Access to or disclosure of ship security records

The master and the company must ensure that all ship security records are—

(a) available to the chief executive and to officers duly authorised by the Designated Authorities of other parties to the Convention to verify that the provisions of the ship security plan are being implemented; and

(b) protected from unauthorised access or disclosure.

Compare: Code, Part A s 10.4, Part B s 10.1

Communication

57 Communication

(1) A company must ensure that effective means are available to notify personnel of changes in security conditions on board the ship.

(2) A company must ensure that there are effective communications systems and procedures to permit continuous communication between the ship security personnel, port facilities interfacing with the ship, ships interfacing with the ship, and national or local authorities with security responsibilities.

(3) Communications systems and procedures must enable ship personnel to notify, in a timely manner, the port facility operator or other ships of a security threat or incident on board.

Control measures

58 Clear grounds for imposing control measures

For the purposes of section 31(1) of the Act, the chief executive has clear grounds to believe that a ship is not in compliance with the requirements of the Act if the chief executive has reasonable grounds for believing that—

(a) the certificate that is produced when required under section 29 of the Act is not valid:

(b) serious deficiencies exist in the ship's security equipment, documentation, or arrangements required by the Act or these regulations:

(c) the ship does not comply with the requirements of the Act or these regulations:

(d) the master or the ship personnel are not familiar with essential shipboard security procedures or cannot carry out drills related to the security of the ship or that such procedures or drills have not been carried out:

(e) key ship personnel are not able to establish proper communications with any other key ship personnel with security responsibilities on board the ship:

(f) the ship—

(i) has embarked persons or loaded stores or goods at a port facility or from another ship where either the port facility or the other ship is in breach of the Act or these regulations; and

(ii) has not completed a declaration of security, or taken appropriate, special, or additional security measures, or maintained appropriate ship security procedures:

(g) the ship—

(i) has embarked persons, or loaded stores or goods at a port facility or from another source where either the port facility or the other source is not required to comply with the Act or these regulations; and

(ii) has not taken appropriate, special, or additional security measures, or has not maintained appropriate security procedures:

(h) if the ship holds a later, consecutively issued interim certificate, the interim certificate was requested to avoid full compliance with the Act or these regulations beyond the period that the interim certificate is valid.

Compare: Code, Part B ss 4.32, 4.33

Part 3
Port facility security

Port facility security levels

59 Commencement level

Unless otherwise directed by the chief executive, every port facility shall operate at security level 1 from 1 July 2004.

60 Security level 1

(1) At security level 1, a port facility operator must carry out through appropriate measures the following activities to identify and take preventive measures against security incidents:

(a) ensure the performance of all port facility security duties; and

(b) control access to the port facility; and

(c) monitor the port facility, including anchoring and berthing areas; and

(d) monitor restricted areas to ensure that access is only granted to persons with appropriate authority; and

(e) supervise the handling of cargo; and

(f) supervise the handling of ship stores; and

(g) ensure that security communications are readily available.

(2) At security level 1, a port facility operator must implement the security measures for security level 1 as specified in their approved port facility security plan.

Compare: Code, Part A s 14.2

61 Security level 2

At security level 2, the additional measures specified in the port facility security plan must be implemented for each activity specified in regulation 60.

Compare: Code, Part A s 14.3

62 Security level 3

At security level 3,—

(a) the further specific measures specified in the port facility security plan must be implemented for each activity specified in regulation 60; and

(b) port facilities must respond to and implement immediately any security instructions given by the chief executive.

Compare: Code, Part A ss 14.4, 14.4.1

Port facility security assessment

63 Port facility security assessment

(1) Every person who carries out a port facility security assessment must have the appropriate skills or qualifications to evaluate the security of the port facility.

(2) Without limiting the matters that a port facility security assessment may include, a port facility security assessment must—

(a) identify and evaluate assets and infrastructure that need protecting; and

(b) identify possible threats to those assets and infrastructure and the likelihood of their occurrence in order to establish and prioritise security measures; and

(c) identify, select, and prioritise countermeasures and procedural changes and their level of effectiveness in reducing vulnerability; and

(d) identify weaknesses, including human factors, in the infrastructure, policies, and procedures.

Compare: Code, Part A ss 15.3, 15.5

Port facility security plan

64 Port facility security plan approval

A port operator must submit—

(a) 1 copy of their port facility security plan to the chief executive for review and approval; and

(b) a letter certifying that the port facility security plan complies with the Act and these regulations.

65 Chief executive to give notice where port facility security plan covers more than 1 port facility

If the chief executive agrees that a port facility security plan may cover more than 1 port facility, he or she must give notice of the arrangement to the International Maritime Organization.

Compare: Code, Part A s 16.9

66 Language used for port facility security plan

A port facility security plan must be written in English.

Compare: Code, Part A s 16.3

67 Matters to be included in port facility security plan

Without limiting the matters that a port facility security plan may contain, a port facility security plan must include the matters specified in Schedule 2.

Compare: Code, Part A ss 16.1, 16.3

68 When port facility security plan may be kept in electronic form

A port facility security plan may be kept in electronic form, in which case it must be protected from unauthorised deletion, destruction, or amendment.

Compare: Code, Part A s 16.7

69 Port facility security plan to be audited

(1) A port facility operator must ensure an audit of the port facility security plan is performed annually, beginning no later than 1 year from the initial date of approval by the chief executive.

(2) The port facility security plan must be audited if there is a change in the facility's ownership or operator, or if there have been modifications to the facility, including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) An audit of the port facility security plan as a result of modifications to the port facility may be limited to those sections of the port facility security plan affected by the modifications.

Compare: Code, Part A s 16.3.13, Part B ss 16.3.5, 16.58, 16.59

70 Audits of port facility security plan to be independent

(1) Port facility personnel who conduct internal audits of the security activities specified in the port facility security plan or who evaluate the implementation

of the port facility security plan must be independent of the activities being audited.

(2) Subclause (1) does not apply if the requirement to be independent is impracticable due to the size and the nature of the port facility.

Compare: Code, Part A s 16.4

Port facility security officer

71 Port facility security officer

(1) A port facility operator must designate a port facility security officer for each port facility.

(2) A person may be designated as the port facility security officer for 1 or more port facilities if the port facilities for which the port facility security officer is responsible are clearly identified.

(3) A port facility operator must ensure that a port facility security officer is given the necessary support to fulfil his or her duties and responsibilities under these regulations.

Compare: Code, Part A ss 17.1, 17.3

72 Duties and responsibilities of port facility security officer

The duties and responsibilities of a port facility security officer include—

(a) conducting an initial comprehensive security survey of the port facility, taking into account the relevant port facility security assessment; and

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

(c) implementing and exercising the port facility security plan; and

(d) undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures; and

(e) recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account relevant changes to the port facility; and

(f) enhancing security awareness and vigilance of the port facility personnel; and

(g) ensuring adequate training has been provided to personnel responsible for the security of the port facility; and

(h) reporting to the relevant authorities and maintaining records of occurrences that threaten the security of the port facility; and

(i) co-ordinating implementation of the port facility security plan with the appropriate company and ship security officer; and

(j) co-ordinating with security services, as appropriate; and

(k) ensuring that standards for personnel responsible for security of the port facility are met; and

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

(m) when requested, assisting a ship security officer to identify persons who seek to board the ship.

Compare: Code, Part A s 17.2

Training, drills, and exercises on port facility security

73 Port facility security officer to have adequate knowledge and training

(1) The port facility operator must ensure that the port facility security officer has an adequate knowledge of, and relevant training in the following matters relating to port facility security if they are applicable:

(a) security administration:

(b) the relevant international conventions, codes, and recommendations:

(c) the relevant New Zealand legislation:

(d) the responsibilities and functions of other security organisations:

(e) the methodology of port facility security assessment:

(f) the methods of ship and port facility security surveys and inspections:

(g) ship and port operations and conditions:

(h) ship and port facility security measures:

(i) emergency preparedness and response and contingency planning:

(j) the instruction techniques for security training and education, including security measures and procedures:

(k) the handling of sensitive security-related information and security-related communications:

(l) current security threats and patterns:

(m) the recognition and detection of weapons, dangerous substances, and dangerous devices:

(n) the recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of people who are likely to threaten security:

(o) the techniques used to circumvent security measures:

(p) security equipment and systems, and their operational limitations:

(q) the methods of conducting audits, inspection, control, and monitoring:

(r) the methods of searches and non-intrusive inspections:

(s) security drills and exercises, including drills and exercises with ships:

(t) the assessment of security drills and exercises.

(2) The port facility operator must ensure that the port facility security officer has completed the standard International Maritime Organization course for port security facility officers.

Compare: Code, Part A s 18.1, Part B s 18.1

74 Port facility personnel with duties and responsibilities for port facility security to have adequate knowledge and training

The port facility operator must ensure that port facility personnel who have duties and responsibilities for port facility security, as described in the port facility security plan,—

(a) understand those duties and responsibilities; and

(b) have the ability to perform those duties and responsibilities; and

(c) have an adequate knowledge of, and receive appropriate training in the following matters relating to port facility security (if applicable):

(i) current security threats and patterns:

(ii) the recognition and detection of weapons, dangerous substances, and devices:

(iii) the recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of people who are likely to threaten security:

(iv) the techniques used to circumvent security measures:

(v) crowd management and control techniques:

(vi) security-related communications:

(vii) the operation of security equipment and systems:

(viii) testing, calibrating, and maintaining security equipment and systems:

(ix) inspection, control, and monitoring techniques:

(x) the methods of searches and non-intrusive inspections.

Compare: Code, Part A s 18.2, Part B s 18.2

75 Port facility personnel not involved in port facility security to be familiar with port facility security plan

The port facility operator must ensure that port facility personnel who do not have duties or responsibilities for port facility security, as described in the port facility security plan, are familiar with the following matters:

(a) the meaning and the requirements of security level 1, security level 2, and security level 3:

(b) the recognition and detection of weapons, dangerous substances, and dangerous devices:

(c) the recognition, on a non-discriminatory basis, of the characteristics and behavioural patterns of people who are likely to threaten security:

(d) the techniques used to circumvent security measures.

Compare: Code, Part B s 18.3

76 Port facility operator to carry out drills

(1) Taking into account the types of operation of the port facility, port facility personnel changes, the type of ship the port facility is serving, and other relevant factors, the port facility operator must ensure the effective implementation of the port facility security plan by carrying out, at least every 3 months, drills that test the separate elements of the port facility security plan.

(2) The drills referred to in subclause (1) must test the separate elements of the port facility security plan and cover all possible threats to the security of the port facility, including, but not limited to, the following types of security incidents:

(a) damage to, or destruction of, the ship or of a port facility (for example, by explosive devices, arson, sabotage, or vandalism):

(b) hijacking or seizure of the ship or of persons on board:

(c) tampering with the cargo, essential ship equipment or systems, or ship stores:

(d) unauthorised access or use, including presence of stowaways:

(e) smuggling weapons or equipment, including weapons of mass destruction:

(f) use of the ship to carry those persons who intend to cause a security incident and their equipment:

(g) use of the ship itself as a weapon or as a means to cause damage or destruction:

(h) blockage of port entrances, locks, approaches, etc:

(i) nuclear, biological, and chemical attack.

Compare: Code, Part A s 18.3, Part B s 18.5

77 Port facility operator to facilitate exercises

(1) The port facility operator must, at least once every calender year (with no more than 18 months between the exercises), facilitate exercises that test communication, co-ordination, resource availability, and response.

(2) The exercises may involve—

(a) representatives of the Designated Authority; and

(b) representatives of the chief executives of the organisations listed in section 59(1)(a)(ii) of the Act; and

(c) the port facility security officer; and

(d) depending on the security and work implications for the New Zealand ships to which the Act applies, the company security officer; and

(e) depending on the security and work implications for the New Zealand ships to which the Act applies, the ship security officer.

(3) The exercises may be—

(a) full scale or live, or both; or

(b) tabletop simulations or seminars, or both; or

(c) combined with other exercises held, such as emergency response or other exercises involving the Designated Authority.

(4) The chief executive may direct that the requirements of subclauses (1) to (3) may alternatively be satisfied by—

(a) participation of the port facility security staff and appropriate port stakeholders in an emergency response or crisis management exercise conducted by another government agency or private sector entity, provided that the exercise addresses components of the port facility security plan; or

(b) an actual increase in security level; or

(c) implementation of enhanced security measures enumerated in the port facility security plan during periods of critical port operations or special events.

(5) Port security drills and exercises must test the proficiency of port facility personnel in assigned security duties at all security levels and the effective implementation of the port facility security plan. They must enable the port facility security officer to identify any related security deficiencies that need to be addressed.

Compare: Code, Part B ss 18.4, 18.6

78 Port facility security officer to participate in exercises and drills

The port facility security officer must ensure the effective co-ordination and implementation of the port facility security plan by participating in drills and exercises under regulations 76 and 77.

Compare: Code, Part A s 18.4

Port security identification

79 Port security identification

(1) For the purpose of controlling access to ships, port facilities, and port security areas, the following credentials are acceptable for the purpose of establishing identity:

(a) a military identification card:

(b) an identification card issued by a New Zealand government department, government agency, or the New Zealand Defence Force:

(c) a driver's licence issued by the Director of Land Transport:

(d) a seafarer's identity document issued by a contracting government or flag state administration:

(e) a valid passport:

(f) an identification credential issued by a port facility operator:

(g) an identification credential issued by a recognised company, union, or trade association:

(h) other forms of identification approved by the chief executive.

(2) Despite subclause (1), the identification listed in subclause (1) is only acceptable if it contains—

(a) the holder's full name; and

(b) the holder's photograph; and

(c) the name of the issuing authority.

(3) The identification must be protected against being tampered with (for example, be laminated).

(4) In regulation (1)(c), **Director of Land Transport** means the Director of Land Transport appointed under section 104A of the Land Transport Management Act 2003.

Regulation 79(1)(c): amended, on 1 April 2021, by section 175(2) of the Land Transport (NZTA) Legislation Amendment Act 2020 (2020 No 48).

Regulation 79(4): inserted, on 1 April 2021, by section 175(2) of the Land Transport (NZTA) Legislation Amendment Act 2020 (2020 No 48).

80 Signs

(1) A port facility operator must, if and as directed by the chief executive, affix signs at the perimeter of the port security area.

(2) The sign or signs must identify the portion of the port that is designated as port security area.

Part 4
Verification and certification for ships

Verifications for ships

81 Verifications for ships

(1) Every New Zealand ship must have—

(a) an initial verification before the ship is put in service or before the International Ship Security Certificate (**certificate**) is first issued; and

(b) a renewal verification at intervals specified by the chief executive, which must not exceed 5 years, unless otherwise provided by these regulations; and

(c) at least 1 intermediate verification; and

(d) any additional verifications as determined by the chief executive.

(2) The chief executive must carry out all verifications for ships.

(3) The chief executive must ensure the completeness and efficiency of every verification for a ship.

(4) The company and master of a ship must ensure that, after its verification, the ship's security system (including any associated security equipment)—

(a) is maintained in accordance with the Act, these regulations, and the approved ship security plan; and

(b) is not altered without the approval of the chief executive.

Compare: Code, Part A s 19.1

82 Initial verification

An initial verification for a New Zealand ship must—

(a) include a complete verification of the ship's security system (including any associated security equipment); and

(b) ensure that the ship's security system (including any associated security equipment) fully complies with the Act, these regulations, and the approved ship security plan; and

(c) ensure that the security system (including any associated security equipment) is in a satisfactory condition and is fit for the service for which the ship is intended.

Compare: Code, Part A s 19.1.1.1

83 Renewal verification

A renewal verification for a New Zealand ship must ensure that the ship's security system (including any associated security equipment)—

(a) fully complies with the Act, these regulations, and the approved ship security plan; and

(b) is in a satisfactory condition and is fit for the service for which the ship is intended.

Compare: Code, Part A s 19.1.1.2

84 Intermediate verification

(1) If only 1 intermediate verification is carried out, the verification must take place between the second and third anniversary date of the certificate.

(2) The intermediate verification must include an inspection of the ship's security system (including any associated security equipment) to ensure that it remains satisfactory for the service for which the ship is intended.

(3) The intermediate verification must be endorsed on the certificate.

Compare: Code, Part A s 19.1.1.3

International Ship Security Certificate

85 Issue of certificate

(1) The chief executive may issue a certificate for a New Zealand ship after an initial verification is completed for the ship.

(2) The chief executive may issue a new certificate or endorse an existing certificate for a ship after a renewal verification is completed for the ship.

Compare: Code, Part A s 19.2

Duration and validity of certificate

86 Duration of certificate

(1) A certificate may be issued for the period specified by the chief executive, which must not exceed 5 years.

(2) If a certificate is issued for a period of less than 5 years, the chief executive may extend the validity of the certificate beyond the expiry date to the maximum 5-year period.

(3) Subclause (2) applies only if the verifications that are required when a certificate is issued for a period of 5 years are carried out.

Compare: Code, Part A ss 19.3.1, 19.3.3

87 Validity of certificate for renewal verification

(1) If a renewal verification is completed within 3 months before the expiry date of the existing certificate, the new certificate is valid from the date of completion of the renewal verification to a date not exceeding 5 years from the date of expiry of the existing certificate.

(2) If a renewal verification is completed more than 3 months before the expiry date of the existing certificate, the new certificate is valid from the date of completion of the renewal verification to a date not exceeding 5 years from the date of completion of the renewal verification.

(3) If a renewal verification is completed after the expiry date of the existing certificate, the new certificate is valid from the date of completion of the renewal verification to a date not exceeding 5 years from the date of expiry of the existing certificate.

(4) If a renewal verification has been completed and a new certificate cannot be issued or placed on board the ship before the expiry date of the existing certificate, the chief executive may endorse the existing certificate.

(5) If the chief executive endorses an existing certificate under subclause (4), the existing certificate is valid for a further period, which must not exceed 5 months from the expiry date of that certificate.

Compare: Code, Part A ss 19.3.2, 19.3.4

88 Validity of certificate for intermediate verification

If an intermediate verification is completed before the period specified in regulation 81(1),—

(a) the expiry date shown on the certificate must be amended by endorsement to a date that must not be more than 3 years after the date on which the intermediate verification was completed; but

(b) the expiry date may remain unchanged if 1 or more additional verifications are carried out so that the maximum 5-year interval between the verifications is not exceeded.

Compare: Code, Part A s 19.3.7

89 Extension of certificate when ship not in port for verification

(1) If a ship's certificate expires and the ship is not in a port for verification, the company must apply to the chief executive for an extension.

(2) The chief executive may grant an extension, which must not exceed 3 months.

(3) The chief executive may grant an extension under subclause (2) only—

(a) for the purpose of allowing the ship to complete its voyage to the port in which it is to be verified; and

(b) if the chief executive considers that it is proper and reasonable to do so.

(4) A ship that is granted an extension must not leave the port in which it is to be verified without a new certificate.

(5) A new certificate issued to a ship that has been granted an extension under this regulation is valid for a period not exceeding 5 years from the expiry date of the existing certificate (excluding the extended period).

Compare: Code, Part A s 19.3.5

90 Extension of certificate for ships engaged on short voyages

(1) A certificate issued to a ship engaged on short voyages that has not already been extended under these regulations may be extended by the chief executive for a period not exceeding 1 month from the date of expiry of the certificate.

(2) Anew certificate issued to a ship that has been granted an extension under this regulation is valid for a period not exceeding 5 years from the date of expiry of the existing certificate (excluding the extended period).

Compare: Code, Part A s 19.3.6

91 When certificate ceases to be valid

A certificate ceases to be valid—

(a) if the relevant verifications are not completed within the periods specified in these regulations; and

(b) if the certificate is not endorsed in accordance with these regulations; and

(c) when a company assumes the responsibility for the operation of a ship not previously operated by that company; and

(d) on transfer of the ship to another State that is a party to the Convention.

Compare: Code, Part A s 19.3.8

Interim International Ship Security Certificate

92 Issue of interim certificate

The chief executive may issue an interim International Ship Security Certificate (**interim certificate**) in the following cases:

(a) in the case of a ship without a certificate, on delivery or before its entry or re-entry into service:

(b) in the case of a transfer of a New Zealand ship to a State that is a party to the Convention:

(c) in the case of a transfer of a ship from a State that is a party to the Convention to New Zealand owners:

(d) when a company assumes the responsibility for the operation of a ship not previously operated by that company.

Compare: Code, Part A ss 19.4.1, 19.4.3

93 Requirements before issuing interim certificates

The chief executive must, before issuing an interim certificate, verify that—

(a) the ship security assessment has been completed in accordance with the Act and these regulations; and

(b) a copy of the ship security plan is on board the ship, has been submitted for review and approval, and is being implemented on the ship; and

(c) the ship has a ship security alert system that complies with the Act and these regulations; and

(d) the company security officer has made arrangements for carrying out an initial verification, and is satisfied that the ship will successfully complete the verification required under regulation 81(1)(a) within 6 months; and

(e) the master, the ship's security officer, and the ship's other personnel who have security duties,—

(i) are familiar with their duties and responsibilities, and with the relevant provisions of the ship security plan; and

(ii) have been provided that information in languages understood by them; and

(f) the ship security officer meets the requirements of these regulations.

Compare: Code, Part A s 19.4.2

94 Duration and validity of interim certificate

(1) An interim certificate is valid for 6 months or until the certificate under regulation 85 is issued (whichever first occurs).

(2) An interim certificate may not be extended.

Compare: Code, Part A s 19.4.4

95 Restrictions on issue of further interim certificate

The chief executive may not issue another interim certificate for a ship after the interim certificate for that ship has expired if the chief executive considers that a purpose of the interim certificate is for the ship or company to avoid complying with the Act or these regulations.

Compare: Code, Part A s 19.4.5

96 Requirements before accepting validity of interim certificate

The chief executive must, before issuing an interim certificate, ensure that all the requirements of regulation 93(b), (d), and (e) have been met.

Compare: Code, Part A s 19.4.6

Schedule 1
Matters to be included in ship security plan

rr 36, 37

The following matters must be included in a ship security plan:

(a) the identification, and 24-hour contact details, of the company security officer responsible for the ship; and

(b) the identification of the ship security officer; and

(c) a description of the duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects; and

(d) a clear statement on the authority of the master, including the master's overriding authority and responsibility to—

(i) make decisions concerning the safety and security of the ship; and

(ii) request the assistance of the company or the Designated Authority of any party to the Convention, as may be necessary; and

(e) the procedures for responding to any security instructions given at security level 3 by the chief executive or the Designated Authority of any party to the Convention; and

(f) the procedures for interfacing with port facility security activities; and

(g) the measures designed to prevent the unauthorised taking on board a ship of—

(i) a firearm, or any other dangerous or offensive weapon or instrument of any kind; or

(ii) any ammunition; or

(iii) an explosive, incendiary, biological, or chemical substance or device, or any other injurious substance or device of any kind, that could be used to endanger the safety of the ship, persons on board the ship, the port security area, or persons in the port security area; and

(h) the identification of all restricted areas; and

(i) the measures to prevent unauthorised access to—

(i) the restricted areas; and

(ii) the ship; and

(j) the procedures for responding to security threats or breaches of security, including a description of how critical operations of the ship or ship-port interface will be maintained; and

(k) the evacuation procedures in case of security threats or breaches of security; and

(l) the procedures for reporting security incidents; and

(m) the location of the ship security alert system activation points; and

(n) the procedures, instructions, and guidance on the use of the ship security alert system, including testing, activation, deactivation, and resetting, and limiting false alerts; and

(o) the procedures for inspecting, testing, calibrating, and maintaining any security equipment on board the ship; and

(p) the frequency of inspecting, testing, calibrating, and maintaining any security equipment on board the ship; and

(q) the procedures for training, drills, and exercises associated with the ship security plan; and

(r) the frequency of the training, drills, and exercises; and

(s) the procedures for auditing the ship's security activities, and the frequency of the audit; and

(t) the procedures for the periodic review of the ship security plan and for updating it; and

(u) the frequency of the periodic review of the ship security plan; and

(v) security measures for all security levels to—

(i) address each vulnerability identified in the ship security assessment; and

(ii) secure any item listed in subclause (g), where that item is authorised to be on the ship; and

(iii) control access to the ship including:

(A) access ladders; and

(B) access gangways; and

(C) access ramps; and

(D) access doors, sidescuttles, windows, and ports; and

(E) mooring lines and anchor chains; and

(F) cranes and hoisting gear; and

(w) the organisational structure of security for the ship.

Compare: Code, Part A ss 6.1, 9.4.1–9.4.18, Part B ss 9.1, 9.2.1, 9.9

Schedule 2
Matters to be included in port facility security plan

r 67

The following matters must be included in a port facility security plan:

(a) the name, and 24-hour contact details, of the port facility security officer; and

(b) the duties of port facility personnel assigned security responsibilities and of other port facility personnel on security aspects; and

(c) the procedures for responding to any security instructions that the chief executive may give at security level 3; and

(d) the procedures for interfacing with ship security activities; and

(e) the measures designed to prevent the unauthorised taking on board a ship or into a port security area of—

(i) a firearm, or any other dangerous or offensive weapon or instrument of any kind; or

(ii) any ammunition; or

(iii) an explosive, incendiary, biological, or chemical substance or device, or any other injurious substance or device of any kind, that could be used to endanger the safety of the ship, persons on board the ship, the port security area, or persons in the port security area; and

(f) the measures designed to prevent unauthorised access to the port facility, to ships moored at the port facility, to restricted areas of the port facility, and to areas of the port facility designated as a port security area under section 45 of the Act; and

(g) the procedures for responding to security threats or breaches of security, including a description of how critical operations of the port facility or ship-port interface will be maintained; and

(h) the evacuation procedures in case of security threats or breaches of security; and

(i) the procedures for reporting security incidents; and

(j) the procedures for assessing the implications of security threats or breaches of security under subclauses (g) and (h) and of security incidents reported under subclause (i) for the continued appropriateness of the relevant parts of the ship security plan; and

(k) the procedures for responding if the ship security alert system of a ship at the port facility is activated; and

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

(m) the procedures for facilitating—

(i) shore leave for ship personnel or personnel changes; and

(ii) access of visitors to the ship, including representatives of seafarers' welfare and labour organisations; and

(n) the procedures and measures by which an exclusion zone declared under section 59 of the Act is maintained; and

(o) the procedures for training, drills, and exercises associated with the port facility security plan; and

(p) the frequency of the training, drills, and exercises referred to in subclause (o); and

(q) the procedures for auditing the port facility security plan, and the frequency of the audit; and

(r) the procedures for evaluating the initial implementation of the port facility security plan to ensure the port facility security plan is adequate; and

(s) the procedures for the periodic review of the port facility security plan and for updating it; and

(t) the frequency of the periodic review of the port facility security plan; and

(u) the measures for ensuring the security of the information contained in the port facility security plan; and

(v) security measures for all security levels to—

(i) secure any item listed in subclause (e), where that item is authorised to be in the port facility; and

(ii) ensure that unaccompanied baggage does not contain any item listed in subclause (e); and

(iii) control access to the port facility by requiring identification as set out in regulation 79; and

(iv) ensure that only people who are authorised to enter the port facility may enter it.

Compare: Code, Part A ss 16.3.1–15

Diane Morcom,
Clerk of the Executive Council.

Issued under the authority of the Legislation Act 2012.
Date of notification in *Gazette*: 3 June 2004.

Reprints notes

1 General

This is a reprint of the Maritime Security Regulations 2004 that incorporates all the amendments to those regulations as at the date of the last amendment to them.

2 Legal status

Reprints are presumed to correctly state, as at the date of the reprint, the law enacted by the principal enactment and by any amendments to that enactment. Section 18 of the Legislation Act 2012 provides that this reprint, published in electronic form, has the status of an official version under section 17 of that Act. A printed version of the reprint produced directly from this official electronic version also has official status.

3 Editorial and format changes

Editorial and format changes to reprints are made using the powers under sections 24 to 26 of the Legislation Act 2012. See also http://www.pco.parliament.govt.nz/editorial-conventions/.

4 Amendments incorporated in this reprint

Land Transport (NZTA) Legislation Amendment Act 2020 (2020 No 48): section 175(2)

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2021