[LEGAL NOTICE NO. 102]

MARITIME TRANSPORT DECREE 2013
(DECREE NO. 20 OF 2013)

Maritime (ISPS Code) Regulations 2014

TABLE OF PROVISIONS

IN exercise of the powers conferred upon me by section 240(1)*(x)* of the Maritime Transport Decree 2013, I hereby make these Regulations—

PART 1—PRELIMINARY

Short title and commencement

1. These Regulations may be cited as the Maritime (ISPS Code) Regulations 2014 and shall come into force on 1st January, 2015.

Purpose

2.—(1) The objective of these Regulations is to establish a national framework amongst government agencies, the Authority and the shipping and port industry to detect, access and take preventative measures against security threats or incidents affecting ships or port facilities in Fiji used in international trade.

(2) These Regulations—

(a) establish the respective roles and responsibilities of all parties concerned for ensuring maritime security, and the early and efficient collation and exchange of security related information; and

(b) provide the methodology for security assessments for plans and procedures to counter changing security levels in Fiji.

Interpretation

3.—(1) In these Regulations, unless the context otherwise requires,—

"Authority" means the Maritime Safety Authority of Fiji;

"Administration" means the government of the State whose Flag the ship is entitled to fly;

"Chief Executive Officer" means the Chief Executive Officer of the Authority unless expressly provided otherwise in these Regulations;

"Chapter" means a chapter of the Convention;

"Company" means the owner of the ship or any other organisation or person such as the manager, or the bareboat charterer, who has assumed the responsibility

for operation of the ship from the ship owner and who, on assuming such responsibility, has agreed to take over all duties and responsibility imposed by these Regulations and the Code;

"CSO" means the Company Security Officer designated by the Company for ensuring that a ship security assessment is carried out; that a SSP is developed, submitted for approval, and thereafter implemented and maintained and for liaison with PFSOs and the SSO;

"Convention" means the International Convention for the Safety of Life at Sea, 1974 as amended;

"Code" means the International Ship and Port Facility Security Code, and includes amendments made to it from time to time;

"Decree" means the Maritime Transport Decree 2013;

"Declaration of Security" means an agreement reached between a ship and either a port facility or another ship with which it interfaces specifying the security measures each will implement;

"Mobile offshore drilling unit" means a mechanically propelled mobile offshore drilling unit, as defined in Chapter IX/1 of the Convention;

"Port Facility" means a location, as determined by the Authority, where ship/port interface takes place, and this includes areas such as anchorage, waiting berths and approaches from seaward;

"PFSO" means the Port Facility Security Officer designated as responsible for the development, implementation, revision and maintenance of the PFSP and for liaison with the SSOs and CSOs;

"PFSP" means the Port Facility Security Plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident;

"RSO" means a Recognised Security Organisation with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorised to carry out an assessment, or a verification, or approval or certification activity required by these Regulations and the Code;

"Security incident" means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high speed craft, or of a port facility or of any ship/port interface or any ship to ship activity;

"Security level" means the qualification of the degree of risk that a security incident will be attempted or will occur;

"Security level 1" (Normal) means the level at which the ship or port facility normally operates with minimum appropriate protective security measures;

"Security level 2" (Heightened) means the level applying for as long as there is a heightened risk of a security incident for which appropriate additional protective security measures shall be maintained;

"Security level 3" (Exceptional) the level applying for the period of time when there is the probable or imminent risk of a security incident for which further specific protective security measures shall be maintained;

"SSO" means the Ship Security Officer on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the SSP and for liaison with the CSO and PFSOs;

"SSP" means the Ship Security Plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident;

"Ship to Ship activity" means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another;

"Ship to Port Interface" means the physical, operational, or notional location in which ships and supporting watercraft engage port facility services.

(2) The term "ship", when used in these Regulations and the Code, includes mobile offshore drilling units and high-speed craft as defined in Chapter XI-2/1.

(3) The term "Contracting Government" in connection with any reference to a port facility, when used in these Regulations, includes a reference to the "Administration".

(4) Terms not otherwise defined in these Regulations shall have the same meaning as the meaning attributed to them in Chapters I and XI-2.

Application

4.—(1) These Regulations apply to—

(a) the following types of ships engaged in international voyages—

(i) passenger ships, including high-speed passenger craft;

(ii) cargo ships, including high-speed craft, of 100 gross tonnage and upwards;

(iii) Fiji ships engaged in international voyages, any ships returning from the high seas and foreign flagged ships in Fiji waters or intending to proceed to a port or facility in Fiji that is subject to these Regulations;

(iv) mobile offshore drilling units; and

(b) port facilities serving such ships engaged in international voyages.

(2) These Regulations do not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

(3) Notwithstanding sub-regulation (1), the Authority shall decide the extent of application of these Regulations to port facilities within Fiji which, although used primarily by ships not engaged in international voyages, which are also required, occasionally, to serve ships arriving or departing on an international voyage.

(4) The Authority shall base its decision, on a port facility security assessment carried out in accordance with these Regulations.

(5) Any decision which the Authority makes shall not compromise the level of security intended to be achieved by Chapter XI-2 as amended or by these Regulations.

(6) Regulations 8 to 18 and 28 to 31 shall apply to companies and ships as specified in Chapter XI-2/4.

(7) Regulations 8 and 20 to 27 shall apply to port facilities as specified in Chapter XI-2/10.

(8) Nothing in these Regulations shall prejudice the rights or obligations of the Republic of Fiji under international law.

PART 2—REPONSIBILITY OF THE AUTHORITY

Certificate of Compliance

5.—(1) The Authority may, upon application and after assessing and verifying a ship, port or port facility under Article 3 of the Code, issue a certificate of compliance to the ship or port or port facility as prescribed in the Code.

(2) The applicant for a certificate of compliance shall pay the fees to the Authority as prescribed in Schedule 2.

Offences and penalties

6.—(1) Any person or owner, operator or agent of a ship, or port or port facility to which the Code applies, that contravenes a provision of these Regulations commits an offence and is liable upon conviction to a fine not exceeding $100,000 or imprisonment for a term not exceeding 10 years or to both.

(2) Offences and penalties under these Regulations are prescribed in Schedule 5.

Responsibilities of the Authority

7.—(1) Subject to the provisions of Chapters XI-2/3 and XI-2/7, the Authority shall set security levels and provide guidance for protection from security incidents.

(2) Higher security levels indicate greater likelihood of occurrence of a security incident and factors to be considered in setting the appropriate security level include—

(a) the degree that the threat information is credible;

(b) the degree that the threat information is corroborated;

(c) the degree that the threat information is specific or imminent; and

(d) the potential consequences of such a security incident.

(3) The Authority, when setting security level 3, shall issue, as necessary, appropriate instructions and shall provide security related information to the ships and port facilities that may be affected.

(4) The Authority may delegate to a RSO certain responsibilities under Chapter XI-2 and these Regulations with the exception of—

(a) setting of the applicable security level;

(b) approving a Port Facility Security Assessment and subsequent amendments to an approved assessment;

(c) determining the port facilities which will be required to designate a PFSO;

(d) approving a PFSP and subsequent amendments to an approved plan;

(e) exercising control and compliance measures pursuant to Chapter XI-2/9; and

(f) establishing the requirements for a Declaration of Security.

(5) The Authority shall, to the extent it considers appropriate, test the effectiveness of the Ship or the Port Facility Security Plans, or of amendments to such plans, it has approved, or, in the case of ships, of ships security plans which have been approved on its behalf.

Declaration of Security

8.—(1) The Authority shall determine when a Declaration of Security is required by sub-regulation (2) by assessing the risk the ship/port interface or ship to ship activity poses to persons, property or the environment.

(2) A ship can request completion of a Declaration of Security when—

(a) the ship is operating at a higher security level than the port facility or another ship it is interfacing with;

(b) there is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;

(c) there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;

(d) the ship is at a port which is not required to have and implement an approved PFSP; or

(e) the ship is conducting ship to ship activities with another ship not required to have and implement an approved SSP.

(3) Requests for the completion of a Declaration of Security under this regulation shall be acknowledged by the applicable port facility or ship.

(4) The Declaration of Security shall be completed by—

(a) the master or the SSO on behalf of the ship;

(b) the PFSO or, if the Authority determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

(5) The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each.

(6) The Authority shall specify, bearing in mind the provisions of Chapter XI- 2/9.2.3 of the Convention, the minimum period for which Declarations of Security shall be kept by the port facilities located within Fiji.

(7) The Authority shall specify, bearing in mind the provisions of Chapter XI-2/9.2.3 of the Convention, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

PART 3—RESPONSIBILITY OF SHIPPING COMPANIES AND SHIPS

Obligation of the Company

9.—(1) The Company shall ensure that the SSP contains a clear statement emphasising the master's authority.

(2) The Company shall establish in the SSP that the master 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 Company or of the Authority as may be necessary.

(3) The Company shall ensure that the CSO, the master and the SSO are given the necessary support to fulfill their duties and responsibilities in accordance with Chapter XI-2 as amended and these Regulations.

Ship Security

10.—(1) A ship is required to act upon the security levels set by the Authority as set in sub-regulations (2), (3) and (4) or as set by the Authority.

(2) At security level 1, the following activities shall be carried out through appropriate measures, on all ships, taking into account the guidance given in Part B of the Code, in order to identify and take preventive measures against security incidents—

(a) ensuring the performance of all ship security duties;

(b) controlling access to the ship;

(c) controlling the embarkation of persons and their effects;

(d) monitoring restricted areas to ensure that only authorised persons have access;

(e) monitoring of deck areas and areas surrounding the ship;

(f) supervising the handling of cargo and ship's stores;

(g) ensuring that security communication is readily available; and

(h) ensure liaison with the Port Facility to ensure designated secure area for inspection and searching of persons, baggage, personal effects, vehicles and contents can take place during embarking or disembarking the ship.

(3) At security level 2, the additional protective measures, specified in the SSP, shall be implemented for each activity detailed in sub-regulation (2), which may include but are not limited to the following elements—

(a) assigning additional personnel to patrol deck areas during silent hours to deter unauthorised access;

(b) limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;

(c) deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols;

(d) establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility;

(e) increasing the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship;

(f) escorting visitors on the ship;

(g) providing additional specific security briefings to all ship personnel on any identified threats, re-emphasising the procedures for reporting suspicious persons, objects, or activities and stressing the need for increased vigilance; and

(h) carrying out a full or partial search of the ship.

(4) At security level 3, further specific protective measures, specified in the SSP, shall be implemented for each activity detailed in sub-regulation (2), which may include but not limited to the following elements—

(a) limiting access to a single, controlled, access point;

(b) granting access only to those responding to the security incident or threat thereof;

(c) directions of persons on board;

(d) suspension of embarkation or disembarkation;

(e) suspension of cargo handling operations and deliveries;

(f) evacuation of the ship;

(g) movement of the ship; and

(h) preparing for a full or partial search of the ship.

(5) Whenever security level 2 or 3 is set by the Authority, the ship shall acknowledge receipt of the instructions on change of the security level.

(6) Prior to entering a port in Fiji or whilst in a port in Fiji that has set security level 2 or 3, a ship shall acknowledge receipt of this instruction as required under sub-regulation (5) above and shall confirm to the PFSO the initiation of the implementation of the appropriate measures and procedures as detailed in the SSP, and in the case of security

level 3, instructions issued by the Authority which has set security level 3. The ship shall report any difficulties in implementation and in such cases, the PFSO and SSO shall liaise and co-ordinate the appropriate actions.

(7) If a ship is required by the Authority to set, or is already at, a higher security level than that set for any port in Fiji it intends to enter or in which it is already located, then the ship shall advise, without delay, to the Authority of the situation and in such cases, the SSO shall liaise with the PFSO and co-ordinate appropriate actions, if necessary.

(8) When the Authority requires ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government, the Authority shall inform that Contracting Government without delay.

(9) When the Authority sets security levels and ensures the provision of security level information to ships operating in Fiji waters, or the ship has communicated its intention to enter into Fiji waters, such ships shall be advised to maintain vigilance and report immediately to the Authority and any nearby coastal States any information that comes to their attention that might affect maritime security in the area.

(10) When advising such ships of the applicable security level, the Authority shall, advise those ships of any security measures that they should take and, if appropriate, of measures that have been taken by the Authority to provide protection against the threat.

Master's discretion

11.—(1) The Master shall not be constrained by the Company, the charterer or any other person from taking or executing any decision which, in the professional judgment of the Master, is necessary to maintain the safety and security of the ship. This includes denial of access to persons (except those identified as duly authorised by the Authority) or their effects and refusal to load cargo, including containers or other closed cargo transport units.

(2) If, in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the Master may give precedence to measures intended to maintain the safety of the ship, and take such temporary security measures as seem best under all circumstances.

Ship Security Assessment

12.—(1) The ship security assessment is an essential and integral part of the process of developing and updating the SSP.

(2) The CSO shall ensure that the ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with this regulation, taking into account the guidance given in Part B of the Code.

(3) Subject to sub-regulation (2), a RSO may carry out the ship security assessment of a specific ship.

(4) The ship security assessment shall include an on-scene security survey and, at least, the following elements—

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

(b) identification and evaluation of key ship board operations that it is important to protect;

(c) identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and

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

(5) The ship security assessment shall be documented, reviewed, accepted and retained by the Company.

Ship Security Plan

13.—(1) Fiji ships on international voyages shall carry on board a SSP approved by the Authority, and the plan shall make provisions for the three security levels as defined in these Regulations.

(2) Subject to regulation 12(2), a RSO may prepare the SSP for a specific ship.

(3) The Authority may entrust the review and approval of SSPs, or of amendments to a previously approved plan, to RSOs.

(4) The RSO undertaking the review and approval of a SSP, or its amendments on behalf of the Authority for a specific ship, shall not have been involved in either the preparation of the ship security assessment or of the SSP, or of the amendments, under review.

(5) The submission of a SSP or of amendments to a previously approved plan for approval shall be accompanied by the security assessment on the basis of which the plan or the amendments have been developed.

(6) Such a plan shall be developed, taking into account the guidance given in Part B of the Code and shall be written in the working language or languages of the ship, and if the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included, and the plan shall address, at least, the following—

(a) measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorised from being taken on board the ship;

(b) identification of the restricted areas and measures for the prevention of unauthorised access to them;

(c) measures for the prevention of unauthorised access to the ship;

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

(e) procedures for responding to any security instructions which may be issued by the Authority for security level 3;

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

(g) duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

(h) procedures for auditing the security activities;

(i) procedures for training, drills and exercises associated with the plan;

(j) procedures for interfacing with port facility security activities;

(k) procedures for the periodic review of the plan and for updating;

(l) procedures for reporting security incidents;

(m) identification of the SSO;

(n) identification of the CSO including 24-hour contact details;

(o) procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;

(p) frequency for testing or calibration of any security equipment provided on board;

(q) identification of the locations where the ship security alert system activation points are provided; and

(r) procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.

(7) Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

(8) The Authority shall determine which changes to an approved SSP or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Authority, and any such changes shall be at least as effective as those measures prescribed in Chapter XI-2 as amended and these Regulations.

(9) The nature of the changes to the SSP or the security equipment that have been specifically approved by the Authority, pursuant to Regulation 11(5), shall be documented in a manner that clearly indicates such approval, and this approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment are reinstated, this documentation no longer needs to be retained by the ship.

(10) The plan may be kept in an electronic format, and in such a case, it shall be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment.

(11) The plan shall be protected from unauthorised access or disclosure.

(12) The SSPs are not subject to inspection by Port State Control Officers duly authorised by a Contracting Government to carry out control and compliance measures in accordance with Chapter XI-2/9, save in circumstances specified in sub-regulation (13).

(13) If the Port State Control Officers duly authorised by a Contracting Government have clear grounds to believe that the ship is not in compliance with the requirements of Chapter XI-2 or Part A of the Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the SSP, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Contracting Government of, or the master of, the ship concerned. Nevertheless, the provisions in the plan relating to sub-regulation (6)*(b), (d), (e), (g), (o), (q) and (r)* are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Administration concerned.

Records and audits

14.—(1) Records of ship's security activities addressed in the SSP, including Declarations of Security and the record of the ship security level, shall be maintained onboard for a period covering at least the previous 10 calls at port facilities or a period specified by the Administration bearing in mind the provisions of Chapter XI-2/9.2.3 as listed below—

(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;

(f) internal audits and reviews of security activities;

(g) periodic review of the ship security assessment;

(h) periodic review of the SSP;

(i) implementation of any amendments to the plan; and

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

(2) The records shall be kept in the working language or languages of the ship, and if the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included.

(3) The records may be kept in an electronic format, and in such a case, they shall be protected by procedures aimed at preventing their unauthorised deletion, destruction or amendment.

(4) The records shall be protected from unauthorised access or disclosure.

Audits

15. SSPs shall be audited at intervals not exceeding 5 years and plans shall be verified annually for compliance by the Authority or approved RSOs.

Company Security Officer

16.—(1) The Company shall designate a CSO and a person designated as the CSO may act as the CSO for one or more ships, depending on the number or types of ships the Company operates provided it is clearly identified for which ships that person is responsible.

(2) A Company may, depending on the number or types of ships they operate, designate several persons as CSOs provided it is clearly identified for which ships each person is responsible.

(3) Shipping companies shall appoint a CSO to implement and administer the requirements of this regulation, subject to the approval of the Chief Executive Officer.

(4) The CSO shall be empowered to—

(a) enter ships to make inquiries, examinations, inspections and searches in accordance with this regulation; and

(b) implement all security measures as required by this regulation.

(5) In addition to those specified elsewhere in these Regulations, the duties and responsibilities of the CSO shall include, but are not limited to—

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

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

(c) ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the SSP;

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

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

(f) arranging for the initial and subsequent verifications of the ship by the Authority or the approved RSO;

(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;

(h) enhancing security awareness and vigilance;

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

(j) ensuring effective communication and co-operation between the SSO and the relevant PFSOs;

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

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

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

(n) ensuring the conduct of ship security drills and exercises;

(o) ensuring the proper maintenance of all records pertaining to the ship's security;

(p) notifying law enforcement agencies and other law enforcement respondents of ship security incidents and any breaches of these Regulations; and

(q) ensuring that all security measures set forth in this regulation are implemented and enforced.

Ship Security Officer

17.—(1) Companies shall appoint a designated SSO aboard each security regulated ship to implement and administer the requirements of this regulation, subject to the approval of the Chief Executive Officer.

(2) The SSO shall be empowered to—

(a) implement various levels of physical security controls aboard assigned security regulated ships; and

(b) implement security measures as required by this regulation.

(3) In addition to those specified elsewhere in these Regulations, the duties and responsibilities of the SSO shall include, but are not limited to—

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

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

(c) coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant PFSOs;

(d) proposing modifications to the SSP;

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

(f) enhancing security awareness and vigilance on board;

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

(h) reporting all security incidents;

(i) coordinating implementation of the SSP with the CSO and the relevant PFSO;

(j) ensuring that security equipment is properly operated, tested, calibrated and maintained, if any;

(k) ensuring the conduct of ship security drills and exercises;

(l) ensuring the proper maintenance of all records pertaining to the ship's security;

(m) notifying the CSO of ship security incidents and any breaches of this regulation. In the absence of a CSO, notify law enforcement agencies and other law enforcement respondents of ship security incidents and any breaches of this regulation; and

(n) ensuring that all security measures set forth in this regulation are implemented and enforced.

Training, drills and exercises on ship security

18.—(1) The CSO and SSO shall have knowledge and have received training in the following areas—

(a) security administration;

(b) relevant international conventions, codes and recommendations;

(c) relevant Government laws;

(d) responsibilities and functions of other security organisations;

(e) ship's security assessment;

(f) ship security surveys and inspections;

(g) ship and port facility security measures;

(h) emergency preparedness and response and contingency planning;

(i) security measures and procedures;

(j) classification of security information;

(k) recognition of security threats and patterns;

(l) overview of ISPS audits;

(m) methods of physical searches and non-intrusive inspections;

(n) security drills and exercises, including drills and exercises with port facilities; and

(o) assessment of security drills and exercises.

(2) Shipboard personnel delegated under the SSP shall have sufficient knowledge and ability to perform the assigned duties.

(3) In order to ensure the effective implementation of the SSP, drills shall be carried out at least every three (3) months.

(4) When 25 per cent of ship's personnel have been changed, with personnel that have not previously participated in any drill on that ship within the last three months, a drill must be conducted within one week of this change, and these drills should test individual elements of the plan.

(5) The CSO may participate in the security exercises in conjunction with relevant Administration, SSO if available, and PFSO, once each calendar year with no more than 18 months intervals in between, to ensure the effective coordination and implementation of SSPs.

(6) These exercises shall test communications, coordination, resource availability, and response and may be—

(a) a full scale or live exercise;

(b) a table top simulation; or

(c) a combined with search and rescue or emergency response exercise.

PART 4—REQUIREMENTS FOR RECOGNISED SECURITY ORGANISATION

Recognised Security Organisation

19.—(1) The Chief Executive Officer may authorise a RSO to undertake certain security related activities on behalf of the State, consisting of the following—

(a) conduct security assessments;

(b) inspect and audit port facilities;

(c) advise or provide assistance on security matters.

(2) The RSO shall not—

(a) set security levels;

(b) approve Security Assessments;

(c) approve Security Plans; or

(d) exercise ship control and compliance measures.

(3) The Chief Executive Officer shall ensure that the RSO has the necessary competencies to perform the delegated duties, and in considering the qualification of approved RSO, the Chief Executive Officer shall ensure that the RSO are able to demonstrate competencies in the following areas—

(a) expertise in relevant aspects of security;

(b) appropriate knowledge of ship and port operations including general knowledge of ship's layout and port layout when providing services for such ships and port facilities;

(c) their capability to assess the likely security risks that could occur during ship and port facility operations including the ship/port interface and the ways to minimise such risks;

(d) training and improving the expertise of their personnel;

(e) screening of their security personnel;

(f) security of documents and sensitive materials;

(g) application of the requirements of Chapter XI-2 as amended and these Regulations and relevant national and international legislation and security requirements;

(h) knowledge of current security threats and patterns;

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

(j) ability to recognise behavioural patterns of persons who are likely to threaten security;

(k) knowledge on techniques used to circumvent security measures; and

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

(4) The Authority may revoke the approval and appointment of RSO's if it fails to meet or maintain the conditions and qualifications set forth in this regulation.

PART 5—REQUIREMENTS FOR PORT FACILITIES

Port facility security

20.—(1) A port facility in Fiji is required to act upon the security levels set by the Authority. Security measures and procedures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, passengers, ship, ship's personnel and visitors, goods and services.

(2) At security level 1, the following activities shall be carried out through appropriate measures in all port facilities, taking into account the guidance given in Part B of the Code, in order to identify and take preventive measures against security incidents—

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

(b) controlling access to the port facility;

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

(d) monitoring restricted areas to ensure that only authorised persons have access;

(e) supervising the handling of cargo;

(f) supervising the handling of ship's stores; and

(g) ensuring that security communication is readily available.

(3) At security level 2, the additional protective measures specified in the PFSP shall be implemented for each activity detailed in sub-regulation (2), taking into account the guidance given in Part B of the Code.

(4) At security level 3, further specific protective measures specified in the PFSP shall be implemented for each activity detailed in sub-regulation (2), taking into account the guidance given in Part B of the Code. In addition, at security level 3, port facilities in Fiji are required to respond to and implement any security instructions given by the Authority.

(5) When a PFSO is advised that a ship encounters difficulties in complying with the requirements of Chapter XI-2 as amended or this regulation or in implementing the appropriate measures and procedures as detailed in the SSP, and in the case of security level 3 following any security instructions given by the Authority, the PFSO and SSO shall liaise and co-ordinate appropriate actions.

(6) When a PFSO is advised that a ship is at a security level, which is higher than that of the port facility, the PFSO shall report the matter to the Authority and shall liaise with the SSO and co-ordinate appropriate actions, if necessary.

Port facility security assessment

21.—(1) The port facility security assessment is an essential and integral part of the process of developing and updating the PFSP.

(2) The port facility security assessment shall be carried out by the Authority, and the Authority may authorise a RSO to carry out the port facility security assessment of a specific port facility in Fiji.

(3) When the port facility security assessment has been carried out by a RSO, the security assessment shall be reviewed and approved for compliance with this regulation by the Authority.

(4) The persons carrying out the assessment shall have appropriate skills to evaluate the security of the port facility in accordance with this regulation, taking into account the following elements—

(a) physical security;

(b) security equipment;

(c) security procedures;

(d) radio communications systems (including IT systems and networks);

(e) transportation infrastructure;

(f) utilities infrastructure;

(g) other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port, port facility or aboard ships adjacent thereto; and

(h) available expert assistance.

(5) The port facility security assessments shall be reviewed and updated, annually taking into account changing threats and/or minor changes in the port facility and shall always be reviewed and updated when major changes to the port facility take place.

(6) The port facility security assessment shall include, at least, the following elements—

(a) identification and evaluation of important assets and infrastructure it is important to protect;

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

(c) identification, selection and prioritisation of counter measures and procedural changes and their level of effectiveness in reducing vulnerability;

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

(e) the Authority may allow a port facility security assessment to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar, and if the Authority allows such an arrangement, it shall communicate to the International Maritime Organization the particulars thereof.

(7) Upon completion of the port facility security assessment, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability, and the report shall be protected from unauthorised access or disclosure.

Port facility security plan

22.—(1) A PFSP shall be developed and maintained, on the basis of a port facility security assessment, for each port facility, adequate for the ship/port interface, and the plan shall make provisions for the three security levels, as defined in this regulation.

(2) Subject to regulation 19 (2), a RSO may prepare the PFSP for a specific port facility.

(3) The PFSP shall be approved by the Authority.

(4) Such a plan shall be developed taking into account the guidance given in Part B of the Code and shall be in the working language of the port facility, and the plan shall address, at least, the following elements—

(a) measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorised, from being introduced into the port facility or on board a ship;

(b) measures designed to prevent unauthorised access to the port facility, to ships moored at the facility, and to restricted areas of the facility;

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

(d) procedures for responding to any security instructions which may be issued by the Authority for security level 3;

(e) procedures for evacuation in case of security threats or breaches of security;

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

(g) procedures for interfacing with ship security activities;

(h) procedures for the periodic review, auditing and updating of the security plan;

(i) procedures for reporting security incidents;

(j) identification of the PFSO including 24-hour contact details;

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

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

(m) procedures for auditing the PFSP;

(n) procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and

(o) procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labour organisations.

(5) Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the port facility.

(6) The PFSP may be combined with, or be part of, the port security plan or any other port emergency plan or plans.

(7) The Authority shall determine which changes to the PFSP shall not be implemented unless the relevant amendments to the plan are approved by them.

(8) The plan may be kept in an electronic format and in such a case, it shall be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment.

(9) The plan shall be protected from unauthorised access or disclosure.

(10) The Authority may allow a PFSP to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar and such an alternative arrangement shall be communicated to the Organization by the Authority.

Port Facility Security Officer

23.—(1) The Chief Executive Officer of a Port Management Company or a Port Facility Operator shall appoint the PFSO.

(2) A PFSO shall be designated for each port facility and may be designated as the PFSO for one or more port facilities.

(3) The PFSO shall be empowered to—

(a) enter port facilities or board ships to make inquiries, examinations, inspections, searches, seizures and apprehend in accordance with this regulation;

(b) exercise control measures over ships within the port and to require Declarations of Security with those ships; and

(c) implement all security measures and protocols as required by this regulation.

(4) The PFSO may delegate any or all of his or her powers and functions under this regulation to qualified security officers.

(5) In addition to those specified elsewhere in these Regulations, the duties and responsibilities of the PFSO shall include, but are not limited to—

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

(b) ensuring the completion and timely audit of required security assessments;

(c) ensuring the development, submission, implementation and timely audit of required security plans;

(d) implementing and exercising the PFSP;

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

(f) conducting port security drills and exercises and submitting report to the Chief Executive Officer;

(g) maintaining all security records for a period of 7 years;

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

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

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

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

(l) coordinating implementation of the PFSP with the appropriate Company and SSOs;

(m) coordinating with security services, as appropriate;

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

(o) ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and

(p) assisting SSOs in confirming the identity of those seeking to board the ship when requested.

Port Security Committee

24.—(1) The PFSO shall convene a Port Security Committee, of not less than five members having an interest in the security of the area and who may be selected from—

(a) law enforcement and emergency response agencies;

(b) maritime industry; and

(c) other port stakeholders having a special competence in maritime security.

(2) The Port Security Committee shall—

(a) identify critical port infrastructure and operations;

(b) identify risks (threats, vulnerabilities, and consequences);

(c) determine mitigation strategies and implementation methods; and

(d) advise and assist the PFSO in developing the Security Assessment and Security Plan.

(3) The Port Security Committee shall be empowered to—

(a) enter port and port facility premises;

(b) inspect port and port facility documents, records and plans;

(c) inspect port and port facility security equipment; and

(d) assist with the planning and execution of port and port facility security exercises.

Security personnel

25.—(1) All port, port facility, shipping company, ships and RSO security personnel shall be subjected to a background records check and police clearance requirements.

(2) Port facility, shipping company and ships security personnel and their families shall declare their interest in RSO's or security equipment manufactures or retailers, and the Authority shall maintain a record of these declarations of interest.

(3) Security Assessment and Security Plans audits shall be conducted by the Authority or an organisation approved by the Authority that is independent of the port facility subject to the assessment or audit.

Training, drills, exercises on port facility security

26.—(1) The PFSO and appropriate port facility security personnel shall have sufficient knowledge, in basic ship and port security and the ISPS Code implementation and administration.

(2) The PFSO and port facility security personnel having specific security duties shall understand their duties and responsibilities for port facility security, as described in the PFSP and shall have training in the following areas—

(a) relevant provisions of the Port/Port Facility/Ship Security Plan;

(b) the relevance and application of security levels;

(c) emergency procedures;

(d) recognition and detection of dangerous substances and devices;

(e) recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

(f) other training specific to their duties.

(3) In order to ensure the effective implementation of the PFSP, drills shall be carried out at least once every 3 months to test all the individual elements of the PFSP. Drills shall take into account the specific threats and responses identified in the Security Assessment and the Security Plan and should test individual elements of the plan.

(4) The Chief Exercise Officer of a Port Management Company or a Port Facility Operator shall ensure that the PFSO carries out security exercises once each calendar year with no more than 18 months between exercises to test the effectiveness of the PFSP, and enable the Security Officer to identify any security related deficiencies that need to be addressed.

(5) Security exercises may be—

(a) full scale or live;

(b) tabletop simulation or seminar; or

(c) combined with other exercises.

Records, audits, review and amendments

27.—(1) The responsible PFSO shall maintain all security records for a period of 7 years.

(2) The PFSP shall be audited internally by the PFSO and externally by external auditors approved by the Authority or by the Authority auditors at intervals not exceeding 5 years.

(3) The PFSP shall be verified annually by the Authority or approved RSO.

(4) The PFSP shall be reviewed, updated or amended according to the procedures in the PFSP by the PFSO, and it should be reviewed—

(a) if the port facility security assessment relating to the port facility is altered;

(b) if the external audit carried out by the Authority or approved RSO identifies failings or outdated procedures in PFSP;

(c) following security incidents or threats thereof involving the port facility; and

(d) following changes in ownership or operational control of the port facility.

(5) The PFSO can recommend appropriate amendments to the approved plan following any review of the plan relating to—

(a) proposed changes to security measures of the port facility; and

(b) the removal, alteration or replacement of any equipment and systems essential for maintaining the security of the port facility.

(6) The amendments referred to in sub-regulation (5) shall be submitted to the Authority for approval.

PART 6—CERTIFICATION OF SHIPS

Verification and Certification for Ships

28.—(1) Each ship to which this regulation applies shall be subject to the verifications specified below—

(a) an initial verification before the ship is put in service or before the certificate required under sub-regulation (2) is issued for the first time, which shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of Chapter XI-2, this regulation and the approved SSP. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of Chapter XI-2 as amended and this regulation, is in satisfactory condition and fit for the service for which the ship is intended;

(b) a renewal verification at intervals specified by the Authority, but not exceeding 5 years, except where Regulation 22(4) is applicable. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of Chapter XI-2 as amended, this regulation and the approved SSP, is in satisfactory condition and fit for the service for which the ship is intended;

(c) an intermediate verification will be carried out between the second and third anniversary date of the certificate. The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate; and

(d) any additional verifications as determined by the Authority.

(2) The verifications of ships shall be carried out by the Authority, and the Authority may, entrust the verifications to a RSO referred to in Chapter XI-2/1 as amended.

(3) In every case, the Authority shall fully guarantee the completeness and efficiency of the verification and shall undertake to ensure the necessary arrangements to satisfy this obligation.

(4) The security system and any associated security equipment of the ship after verification shall be maintained to conform with the provisions of Chapter XI-2/4.2 and XI-2/6 (Ships Security Alert System), this regulation and the approved SSP. After any verification under sub-regulation (1) has been completed, no changes shall be made in security system and in any associated security equipment or the approved SSP without the sanction of the Authority.

Issue or endorsement of certificate

29.—(1) An International Ship Security Certificate shall be issued after the initial or renewal verification in accordance with regulation 28(1).

(2) Such certificate shall be issued or endorsed either by the Authority or by an RSO acting on behalf of the Authority.

(3) The Authority may request another Contracting Government, to carry out verification and, if satisfied that regulation 28(1) are complied with, shall issue or authorise the issue of an International Ship Security Certificate to the ship and, where appropriate, endorse or authorise the endorsement of that certificate on the ship, in accordance with this regulation—

(a) a copy of the certificate and a copy of the verification report shall be transmitted as soon as possible to the Authority;

(b) the certificate issued shall contain a statement to the effect that it has been issued at the request of the Authority. The Certificate shall have the same force and receive the same recognition as the certificate issued under sub-regulation (1).

(4) The International Ship Security Certificate shall be issued in accordance with the schedules to these Regulations.

Duration and validity of certificate

30.—(1) The International Ship Security Certificate shall be issued for a period determined by the Authority or a recognised security organisation and shall not exceed 5 years.

(2) When the renewal verification is completed within 3 months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the verification to a date not exceeding 5 years from the date of expiry of the existing certificate—

(a) when the renewal verification is completed after the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the verification to a date not exceeding 5 years from the date of expiry of the existing certificate;

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

(3) If the Authority or the RSO issues a certificate for a period of less than 5 years, the Authority or RSO may extend the validity of the certificate beyond the expiry date to the maximum 5 year period specified in sub-regulation (1).

(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 Authority or RSO acting on behalf of the Authority may endorse the existing certificate and such a certificate shall be accepted as valid for a further period which shall not exceed 5 months from the expiry date.

(5) If a ship at the time when a certificate expires is not in a port in which it is to be verified, the Authority or RSO may extend the period of validity of the certificate but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is to be verified, and then only in cases where it appears proper and reasonable to do so.

(6) No certificate shall be extended for a period longer than 3 months, and the ship to which an extension is granted shall not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new certificate.

(7) When the renewal verification is completed, the new certificate shall be valid to a date not exceeding 5 years from the expiry date of the existing certificate before the extension was granted.

(8) A certificate issued to a ship engaged on short voyages which has not been extended under the foregoing provisions of this regulation may be extended by the Authority or the RSO in consultation with the Authority for a maximum grace period of one month from the date of expiry stated on it.

(9) When the renewal verification is completed, the new certificate shall be valid to a date not exceeding 5 years from the date of expiry of the existing certificate before the extension was granted.

(10) If an intermediate verification is completed before the period specified in regulation 28(1)*(c)*, then—

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

(b) the expiry date may remain unchanged provided one or more additional verifications are carried out so that the maximum intervals between the verifications prescribed by regulation 28(1) are not exceeded.

(11) A certificate issued under regulation 28 shall cease to be valid in any of the following cases—

(a) if the relevant verifications are not completed within the periods specified under regulation 28(1);

(b) if the certificate is not endorsed in accordance with regulation 28(1)*(c)* and sub-regulation (10)*(a)*, if applicable;

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

(d) upon transfer of the ship to the flag of another State.

(12) In the case of—

(a) a transfer of a Fiji ship to the flag of another Contracting Government, the Authority shall, as soon as possible, transmit to the receiving Administration copies of, or all information relating to, the International Ship Security Certificate carried by the ship before the transfer and copies of available verification reports; or

(b) a Company that assumes responsibility for the operation of a ship not previously operated by that Company, the previous Company shall as soon as possible, transmit to the receiving Company copies of any information related to the International Ship Security Certificate or to facilitate the verifications described in regulation 28.

Interim certification

31.—(1) The certificates specified in regulation 29 shall be issued only when the Authority is fully satisfied that the ship complies with the requirements of regulation 29(1), but after 1st July, 2004, for the purposes of—

(a) a Fiji ship without a certificate, on delivery or prior to its entry or re-entry into service;

(b) transfer of a Fiji ship to the flag of another Contracting Government;

(c) transfer of a Fiji ship to the Flag of a non-Contracting Government; or

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

until the certificate referred to in regulation 29(1) is issued, the Authority may cause an Interim International Ship Security Certificate to be issued in accordance with this regulation.

(2) An Interim International Ship Security Certificate shall only be issued when the Authority or the RSO on behalf of the Authority, has verified that—

(a) the ship security assessment required by these Regulations has been completed;

(b) a copy of the SSP meeting the requirements of Chapter XI-2 and these Regulations is provided on board, has been submitted for review and approval, and is being implemented on the ship;

(c) the ship is provided with a ship security alert system meeting the requirements of Chapter XI-2/6, if required;

(d) the CSO—

(i) has ensured—

(A) the review of the SSP for compliance with this regulation;

(B) that the plan has been submitted for approval;

(C) that the plan is being implemented on the ship; and

(ii) has established the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the CSO is satisfied that the ship will successfully complete the required verification in accordance with regulation 28(1)*(a)*, within 6 months;

(e) arrangements have been made for carrying out the required verifications under regulation 28(1)*(a)*;

(f) the master, the SSO and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in this regulation, and with the relevant provisions of the SSP placed on board, and have provided such information in the English language and the working language of the ship's personnel or languages understood by them; and

(g) the SSO meets the requirements of this regulation.

(3) An Interim International Ship Security Certificate shall be valid for 6 months, or until the certificate required by regulation 29 is issued, whichever comes first, and may not be extended.

(4) The Authority shall not cause a subsequent, consecutive Interim International Ship Security Certificate to be issued to a ship if, in the judgment of the Authority or the RSO in consultation with the Authority, one of the purposes of the ship or a Company in requesting such certificate is to avoid full compliance with Chapter XI-2 as amended and these Regulations beyond the period of the initial interim certificate as specified in sub-regulation (3).

(5) For the purposes of Chapter XI-2/9 (Control and Compliance Measures for Ships), the Authority may, prior to accepting an Interim International Ship Security Certificate as a valid certificate, ensure that the requirements of sub-regulation (2)*(d)*, *(e)* and *(f)* have been met.

PART 7—MISCELLANEOUS

Repeal

32. The Marine (ISPS Code) Regulations 2008 is hereby repealed.

Made this 14th day of December 2014.

P. TIKODUADUA
Minister for Infrastructure and Transport

———

SCHEDULE 1

Form of the International Ship Security Certificate

INTERNATIONAL SHIP SECURITY CERTIFICATE

Certificate No.

Issued under the provisions of the
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS
AND OF PORT FACILITIES
(ISPS CODE)

Under the authority of the GOVERNMENT OF FIJI by the Maritime Safety Authority of Fiji

Name of ship: .....

Distinctive number or letters: .....

Port of registry: .....

Type of ship: .....

Gross tonnage: .....

IMO Number: .....

Name and address of the Company: .....

THIS IS TO CERTIFY—

1.0 That the security system and any associated security equipment of the ship has been verified in accordance with Section 19.1 of Part A of the ISPS Code;

2.0 That the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code;

3.0 That the ship is provided with an approved Ship Security Plan.

Date of initial/renewal verification on which this certificate is based: .....

This Certificate is valid until .....
subject to verifications in accordance with section 19.1.1 of Part A of the ISPS Code.

Issued at: ..... Date of issue: .....
(Place of issue of the Certificate)

.....
(*Signature of the duly authorised
official issuing the Certificate)

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT FOR INTERMEDIATE VERIFICATION

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1.1 of Part A of the ISPS Code, the ship was found to comply with the relevant provisions of chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code.

Intermediate verification
Signed: .....
(*Signature of authorised official)
Place: .....
Date: .....

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT FOR ADDITIONAL VERIFICATIONS**

Additional verification
Signed: .....
(*Signature of authorised official)
Place: .....
Date: .....

Additional verification
Signed: .....
(*Signature of authorised official)
Place: .....
Date: .....

Additional verification
Signed: .....
(*Signature of authorised official)
Place: .....
Date: .....

*(**This part of the certificate shall be adapted by the Authority to indicate whether it has established additional verifications as provided for in section 19.1.1.4 of Part A of the ISPS Code)*

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ADDITIONAL VERIFICATION IN ACCORDANCE WITH SECTION A/19.3.7.2 OF THE ISPS CODE

THIS IS TO CERTIFY that at an additional verification required by section 19.3.7.2 of Part A of the ISPS Code, the ship was found to comply with the relevant provisions of chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code.

Signed: .....
(*Signature of authorised official)
Place: .....
Date: .....

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT TO EXTEND THE CERTIFICATE IF VALID FOR LESS THAN 5 YEARS WHERE SECTION A/19.3.3 OF THE ISPS CODE APPLIES

The ship complies with the relevant provisions of Part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.3 of Part A of the ISPS Code, be accepted as valid until ……..

Signed: .....
(*Signature of authorised official)
Place: .....
Date: .....

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT WHERE THE RENEWAL VERIFICATION HAS BEEN COMPLETED AND SECTION A/19.3.4 OF THE ISPS CODE APPLIES

The ship complies with the relevant provisions of Part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.4 of Part A of the ISPS Code, be accepted as valid until ……

Signed: .....
(*Signature of authorised official)
Place: .....
Date: .....

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT TO EXTEND THE VALIDITY OF THE CERTIFICATE UNTIL REACHING THE PORT OF VERIFICATION WHERE SECTION A/19.3.5 OF THE ISPS CODE APPLIES OR FOR A PERIOD OF GRACE WHERE SECTION A/19.3.6 OF THE ISPS CODE APPLIES

This Certificate shall, in accordance with section 19.3.5 / 19.3.6 (delete where appropriate) of Part A of the ISPS Code, be accepted as valid until……..

Signed: .....
(*Signature of authorised official)
Place: .....
Date: .....

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

ENDORSEMENT FOR ADVANCEMENT OF EXPIRY DATE WHERE SECTION A/19.3.7.1 OF THE ISPS CODE APPLIES

In accordance with section 19.3.7.1 of Part A of the ISPS Code, the new expiry date** is ……

Signed: .....
(*Signature of authorised official)
Place: .....
Date: .....

*(**In case of completion of this part of the certificate, the expiry date shown on the front of the Certificate shall also be amended accordingly)*

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

SCHEDULE 2

Form of the Interim International Ship Security Certificate

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

Certificate No.

Issued under the provisions of the
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS
AND OF PORT FACILITIES
(ISPS CODE)

Under the authority of the GOVERNMENT OF FIJI by the Maritime Safety Authority of Fiji

Name of ship: .....
Distinctive number or letters:.....
Port of registry: .....
Type of ship: .....
Gross tonnage: .....
IMO Number:.....
Name and address of the Company: .....
Is this a subsequent, consecutive interim certificate? Yes/No .....
If Yes, date of issue of initial interim certificate: .....

THIS IS TO CERTIFY THAT the requirements of section A/19.4.2 of the ISPS Code have been complied with.

This Certificate is issued pursuant to section A/19.4 of the ISPS Code.

This Certificate is valid until .....

Issued at:..... Date of issue:.....
(Place of issue of the Certificate)

……..
(*Signature of the duly authorised
official issuing the Certificate)

*(*Seal or stamp of issuing authority, as appropriate, must be affixed)*

SCHEDULE 3

Form of a Declaration of Security between a ship and a port facility

DECLARATION OF SECURITY

Name of Ship:	
Port of Registry:	
IMO Number:	
Name of Port Facility:	

This Declaration of Security is valid from …… until ……., for the following activities (list the activities with relevant details)—

.....
.....
.....
.....

under the following security levels—

Security level(s) for the ship:	
Security level(s) for the port facility:	

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Code for the Security of Ships and of Port Facilities.

	The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by—	
Activity	*Port facility*	*Ship*
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorised personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		

Handling of cargo		
Delivery of ship's stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and Part A of Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at …… on the …… day of ……., 20……

Signed for and on behalf of	
Port facility:	Ship:

(Signature of Port Facility Security Officer) (Signature of Master or Ship Security Officer)

Name and title of person who signed	
Name:	Name:
Title:	Title:

*(*This form of Declaration of Security is for use between a ship and a port facility. If the Declaration of Security is to cover two ships, this model should be appropriately modified)*

Contact Details (to be completed as appropriate) (indicate the telephone numbers or the radio channels or frequencies to be used)	
For the port facility:	For the ship:

Port Facility
Port Facility Security Officer
Company
Company Security Officer

Master
Ship Security Officer

SCHEDULE 4

Form of a Statement of Compliance of a Port Facility

STATEMENT OF COMPLIANCE OF A PORT FACILITY

Statement Number

Issued under the provisions of Part B of the
INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES (ISPS CODE)

THE GOVERNMENT OF FIJI
Maritime Safety Authority of Fiji

Name of the Port Facility: .....
Address of the Port Facility: .....

THIS IS TO CERTIFY that the compliance of this port facility with the provisions of chapter XI-2 and Part A of the International Code for the Security of Ships and of Port Facilities (ISPS Code) has been verified and that this port facility operates in accordance with the approved Port Facility Security Plan. This plan has been approved for the following <specify the types of operations, types of ship or activities or other relevant information> (delete as appropriate):

Passenger ship
Passenger high speed craft
Cargo high speed craft
Bulk carrier
Oil tanker
Chemical tanker
Gas carrier
Mobile offshore Drilling Units
Cargo ships other than those referred to above

This Statement of Compliance is valid until ....., subject to verifications (as indicated overleaf)

Issued at..... .....
(place of issue of the statement)

Date of issue..... .....
(Signature of the duly authorised official issuing the document)

(Seal or stamp of issuing authority, as appropriate)

ENDORSEMENT FOR VERIFICATIONS

The Government of (insert name of the State) has established that the validity of this Statement of Compliance is subject to {insert relevant details of the verifications (e.g. mandatory annual or unscheduled)}.

THIS IS TO CERTIFY that, during a verification carried out in accordance with paragraph B/16.62.4 of the ISPS Code, the port facility was found to comply with the relevant provisions of chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code.

1ST VERIFICATION Signed: .....
(Signature of authorised official)
Place: .....
Date: .....

2ND VERIFICATION Signed: .....
(Signature of authorised official)
Place: .....
Date: .....

3RD VERIFICATION Signed: .....
(Signature of authorised official)
Place: .....
Date: .....

4TH VERIFICATION Signed: .....
(Signature of authorised official)
Place: .....
Date: .....

SCHEDULE 5
(Regulation 6)

FINES AND PENALTIES

The following are the list of offences and their respective penalties under these Regulations.

A. Administrative Offences

1. Failure to implement and maintain security plan
2. Failure to conduct training, drills and exercises
3. Failure to implement and maintain physical security measures
4. Failure to implement and maintain operational security measures
5. Failure to maintain security records
6. Failure to meet audit requirements
7. Operating or servicing ships without valid ISSC
8. Failure of a ship to comply with security directions
9. Failure to maintain SSAS/AIS/LRIT
10. Prohibited RSO action

B. Criminal Offences

11. Failure of an individual to comply with security directions
12. Interference with law enforcement or security personnel
13. Trespass
14. Tampering
15. Possession of weapon
16. Endangering persons or property
17. Interference with port facilities or vessels
18. Threat
19. False reporting
20. Counterfeiting
21. Unauthorised disclosure
22. Conflicts of interest
23. Bribery
24. Misuse of official information
25. Security violations

1.0 Application

Individuals and regulated entities (i.e., ships, corporations, contractors, organisations and port facilities) may be held administratively or criminally liable for violations of ship and port security laws and regulations. Attempt or conspiracy to commit a violation constitutes a violation of the underlying offence.

Administrative Offences

2.0 Failure to implement and maintain security plan.

It shall be an administrative offence for a regulated entity to operate without a valid security plan as required by law, punishable by—

a. $100,000 fine per day of violation;

b. Facility closure;

c. Ship seizure and detention; and

d. Operating License/International Ship Security Certificate/Statement of Compliance revocation.

3.0 Failure to conduct training, drills and exercises

It shall be an administrative offence for a regulated entity to fail to conduct training, drills and exercises as required by law, punishable by—

a. $50,000 fine per day of violation;

b. Facility closure;

c. Ship seizure and detention; and

d. Operating License/International Ship Security Certificate/Statement of Compliance revocation.

4.0 Failure to implement and maintain physical security measures

It shall be an administrative offence for a regulated entity to fail to implement and maintain all physical security measures as required by the security plan, punishable by—

a. $50,000 fine per day of violation;

b. Facility closure;

c. Ship seizure and detention; and

d. Operating License/International Ship Security Certificate/Statement of Compliance revocation.

5.0 Failure to implement and maintain operational security measures

It shall be an administrative offence for a regulated entity to fail to implement and maintain all operational security measures as required by the port facility security plan, punishable by—

a. $50,000 fine per day of violation;

b. Facility closure;

c. Ship seizure and detention; and

d. Operating License/International Ship Security Certificate/Statement of Compliance revocation.

6.0 Failure to maintain security records

It shall be an administrative offence for a regulated entity to fail to maintain security records as required by law, punishable by—

a. $50,000 fine per day of violation;

b. Facility closure;

c. Ship seizure and detention; and

d. Operating License/International Ship Security Certificate/Statement of Compliance revocation.

7.0 Failure to meet audit requirements

It shall be an administrative offence for a regulated entity to fail to meet audit requirements as required by law, punishable by—

a. $25,000 fine per day of violation;

b. Facility closure;

c. Ship seizure and detention; and

d. Operating License/International Ship Security Certificate/Statement of Compliance revocation.

8.0 Operating or servicing ships without valid International Ship Security Certificates

It shall be an administrative office for a regulated entity to operate or service a regulated ship that does not possess a valid International Ship Security Certificate (ISSC), punishable by—

a. $100,000 fine per violation;

b. Facility closure;

c. Ship seizure and detention; and

d. Operating License/Statement of Compliance revocation.

9.0 Failure of a ship to comply with security directions.

It shall be an administrative offence for any ship or small commercial or recreational boat to fail to comply with security directions issued by the Administration punishable by—

a. $50,000 fine per violation;

b. Ship/boat seizure and detention; and

c. International Ship Security Certificate/Statement of Compliance revocation.

10.0 Failure to maintain SSAS and /AIS

It shall be an administrative offence for a regulated ship to fail to maintain its Ship's Security Alert System (SSAS)/Automated Identification System (AIS) as required by law, punishable by—

a. $50,000 fine per day of violation;

b. Ship seizure and detention; and

c. International Ship Security Certificate/Statement of Compliance revocation.

11.0 Prohibited RSO actions

It shall be an administrative offence for a Recognised Security Organization (RSO) to set security levels, approve ship or port facility security assessments, approve ship security plans without the Administration's approval or port facility security plans, or exercise ship control and compliance measures. A violation under this section is punishable by—

a. $50,000 fine per violation; and

b. Revocation of RSO certification.

Criminal Offences

12.0 Failure of an individual to comply with security directions

It shall be a criminal offence for an individual to knowingly or intentionally fail to comply with security directions issued by the Administration, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

13.0 Interference with law enforcement or security personnel

It shall be a criminal offence for an individual to knowingly or intentionally prevent, obstruct, resist or otherwise delay law enforcement or ship/port security personnel in the discharge of their duties, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

14.0 Trespass

It shall be a criminal offence for an individual to knowingly or intentionally enter or remain on or in a regulated port facility, regulated ship or security zone, without the consent of the owner or regulating authority, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

15.0 Tampering

It shall be a criminal offence for an individual to knowingly or intentionally alter, destroy, remove, or manipulate regulated ship or port facility property and containers and cargoes therein without authorisation, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

16.0 Possession of weapon

It shall be a criminal offence for an unauthorised individual to possess a weapon inside a regulated port facility, onboard a regulated ship or within a security zone, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

17.0 Endangering persons or property

It shall be a criminal offence for an individual to knowingly or intentionally endanger persons or property inside a regulated port facility, onboard a regulated ship or within a security zone, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

18.0 Interference with Port Facilities or Vessels

It shall be a criminal offence for an individual to knowingly or intentionally interfere with the operation of a regulated port facility or regulated ships within regulated port facilities or security zones, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

19.0 Threat

It shall be a criminal offence for an individual to knowingly or intentionally communicate the threat of injury to persons or damage to property inside a regulated port facility, onboard a regulated ship or within a security zone, punishable by—

a. $15,000 fine per violation; or

b. Ten years imprisonment.

20.0 False reporting

It shall be a criminal offence for an individual to knowingly or intentionally falsely report the threat of injury to persons or damage to property inside a regulated port facility, onboard a regulated ship or within a security zone, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

21.0 Counterfeiting

It shall be a criminal offence for an individual to knowingly or intentionally forge, counterfeit, or alter without authorisation any security-related certification or documentation, or to use, possess, or exhibit the same, punishable by—

a. $15,000 fine per violation; or

b. Seven years imprisonment.

22.0 Unauthorised disclosure

It shall be a criminal offence for an individual to knowingly or intentionally disclose port facility security assessments, port facility security plans, ship security assessments or ship security plans without authorisation, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

23.0 Conflicts of interest

It shall be a criminal offence for a governmental or port security official to possess an ownership interest in the ports, ships, or recognised security organisations over which he or she exercises regulatory authority, or to confer an unjust benefit to family and/or associates, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

24.0 Bribery

It shall be a criminal offence for a governmental or port security official to knowingly or intentionally solicit or accept money, gifts or favors from a person or an entity seeking action by the official's office or agency, punishable by—

a. $15,000 fine per violation; or

b. Ten years imprisonment.

25.0 Misuse of official information

It shall be a criminal offence for a governmental or port security official to knowingly or intentionally use official information to acquire or aid another to acquire a pecuniary interest in any property, transaction, or enterprise that may be affected by the information, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

26.0 Security violations

It shall be a criminal offence for an individual to knowingly or intentionally violate any security-related law, regulation, rule or order applicable to regulated ships and port facilities, punishable by—

a. $15,000 fine per violation; or

b. Two years imprisonment.

SCHEDULE 6
(Regulation 5)

FEES AND CHARGES FOR AUDIT OF PORT FACILITIES AND SHIPS

Item	*Prescribed Fees*	*Rate $ (VAT Exclusive)*
a.	Initial audit of port facilities	5000
b.	Annual verification audit of port facilities	2000
c	Initial audit for ships	500
d.	Annual verification audit for ships	200
e.	Application, assessing and issuance of certificates for port facilities and ships	200

Cost of transportation, meals and accommodations for Auditors shall be borne by the operators of Port facilities and ship owners and operators.

[LEGAL NOTICE NO. 103]

SHIP REGISTRATION DECREE 2013
(DECREE NO. 19 OF 2013)

Maritime (Ship Registration) Regulations 2014

TABLE OF CONTENTS