MARITIME SECURITY REGULATIONS 2004

Arrangement

Maritime Security Regulations 2004

PURSUANT to section 21 of the Niue Island General Laws Act 1968 and , for the purpose of implementing the International Code for the Security of Ships and of Port Facilities (ISPS Code) under the International Convention for Safety of Life at Sea (SOLAS) Cabinet makes the following regulations:

1 Short Title and Commencement

(1) These Regulations may be cited as the Marine Security Regulations, 2004.

(2) These Regulations come into force on 1st July 2004.

2 Interpretation

(1) In these regulations, unless the context otherwise requires -

"authorised person" means a person with powers and duties under these Regulations;

"**Committee**" means the Maritime Security Committee established under Regulation 5;

"**Company**" means the owner or operator of a vessel to which these Regulations apply;

"Company Security Officer" means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with port facility security officers and the ship security officer;

"Contracting Government" includes the Port Authority;

"**Convention**" means the International Convention for the Safety of Life at Sea, 1974 and its amendments (SOLAS);

"**Deadweight Tonnage**" means the total load of cargo, fuel, stores and ballast that a ship can carry;

"**Department**" means the department of Government with particular responsibility for Port Services and Shipping;

"**Disallowed item**" means

(a) any thing made or altered for use for causing bodily injury or intended by the person who has the article for such use, any article capable of being used for causing bodily injury, any anaesthetising or other substance produced for use for disabling persons or intended by the person who the substance for such use, and

(b) any thing capable of destroying or causing damage to or endangering the safety of a ship, port or port facility or persons on a ship or at a port or port facility, and

(c) any thing likely to destroy or cause damage to or endanger the safety of a ship, port or port facility or persons on a ship or at a port or port facility.

"**Gross Registered Tonnage**" means the total capacity of a vessel in tonnage units of 100 cubic feet;

"**Exclusion Zone**" means a waterside area to which access is temporarily restricted to persons authorised by the Ports Authority;

"**Facility Operator**" means port facility to which these Regulations apply;

"**ISPS Code**" means the International Ship and Port Facility Security Code;

"**Master**" means a person having command or charge of a ship;

"**Maritime Security Committee**" means the committee constituted under Regulation 5;

"**Minister**" means the Minister responsible for National Security;
"**Niue port**" means a port in Niue that service ships engaged on international voyages;
"**Niue ship**" mean a ships that is registered in Niue;
"**Port Authority**" means the Port Authority or the Agency of the Executive Government of Niue responsible for the administration, management and operation of Niue ports and is, for the purposes of the ISPS Code, the Designated Authority;

"**Port Facility**" means the ship/port interface facility that provides for the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship;

"**Port Facility Operator**" means the manager of ship/port interface facility that provides for the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship;

"**Port Facility Security Officer**" means a suitably qualified person designated by the facility operator responsible for the development, implementation, review and maintenance of the Port Facility Security Plan and for liaison with ship security officers, the company security officer and the port security officer;

"**Port Facility Security Plan**" means a plan developed to ensure the application of measures designed to protect any or all of 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;

"**Port Security Plan**" means a plan developed to ensure the application of measures designed to protect any of the port facilities of Niue or all of the port, and ships, persons, cargo, cargo transport units and ship's stores within the those port facilities or ports from the risks of a security incident and incorporates all port facility security plans;

"**Port Security Officer**" (PSO) means a person designated as such by the port authority;

"**Restricted Areas**" means areas on a ship to which access is restricted to crew, persons invited by the master or ship security officer and persons authorised pursuant to these regulations;

"**Restricted Zone**" means landside areas to which access is restricted to persons authorised by the facility operator or persons authorised pursuant to these regulations;

"**Screener**" means a person, approved by the PSO, who conducts screening procedures;

"**Screening Procedures**" means those measures involved in the inspection of people and goods, and the checking for disallowed items;

"**Security Level 1**" means the level for which minimum appropriate protective security measures shall be maintained at all times;

"**Security Level 2**" means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident;

"**Security Level 3**" means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target;

"**Ship Security Officer**" means the person on board a ship, accountable to the master, designated by the Company as responsible for the security of the ship, who shall perform those duties stipulated in the ISPS Code, including implementation and maintenance of the SSP, and liaison with the CSO and PSOs;

"**Ship Security Plan**" means a 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.

"**Sterile Area**" means an area of the port approved pursuant to these regulations in which persons, vehicles and goods are not permitted until given clearance by an authorised person;

"**Unaccompanied Baggage**" means any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of screening;

"**Unlawful Interference**" includes without lawful excuse:

(a) seizing, or exercising control of, a ship by force, or threat of force, or any other form of intimidation;

(b) damaging or destroying a ship that is in service;

(c) placing, or causing to be placed, on board a ship in service a thing that is likely to:

(i) destroy the ship; or

(ii) endanger its safety;

(d) communicating information, which is known to be false, thereby endangering the safety of a ship;

(e) committing an act of violence against a person, property or the environment at a port, if the act:

(i) causes, or is likely to cause, injury or death; and

(ii) endangers, or is likely to endanger, the safe and efficient operation of the port or the safety of anyone at the port;

(f) attempting to commit an act described in any of the above paragraphs.

(2) Terms not otherwise defined in this part shall have the same meaning as the meaning attributed to them in SOLAS.

(3) The following acronyms mean:

CSO	Company Security Officer
DWT	Dead Weight Tonnage
GRT	Gross Registered Tonnage
ISPS Code	International Ship and Port Facility Security Code
MSC	Maritime Security Committee
PFO	Port Facility Officer
PFSA	Port Facility Security Assessment
PFSO	Port Facility Security Officer
PFSP	Port Facility Security Plan
PSA	Port Security Assessment
PSO	Port Security Officer
PSP	Port Security Plan
RSO	Registered Security Organization
SSA	Ship Security Assessment
SSO	Ship Security Officer
SSP	Ship Security Plan

3 Application

(1) These Regulations apply to -

(a) Niue ships;

(b) Niue ports and port facilities; and

(c) all foreign vessels in Niue's waters to which the Convention applies.

(d) fishing vessels 12 metres in length and above fishing in the EEZ of Niue and international waters.

4 Port Security Officer's Duties

The PSO is responsible for:

(a) initiating, developing, promoting and reviewing maritime security policy, legislation, standards and procedures;

(b) auditing and pursuing compliance with maritime security policy, legislation, standards and procedures;

(c) preparing Port Security Plans;

(d) drawing up and maintaining a list of vulnerable points of the ports, including essential equipment/facilities and review their security from time to time;

(e) promote security awareness amongst port workers/users and shipowners;

(f) coordinating the maritime security policy response to a threat or act, which threatens the security of the maritime transport sector;

(g) coordinating the provision of intelligence and information on threats to the maritime industry;

(h) facilitating the development, implementation, review and maintenance of the port security plan and liaison with port facility security officers and ship security officers, where appropriate;

(i) in consultation with PFSOs, ensuring that appropriate security measures are maintained at the port;

(j) maintaining and supervising the implementation of the PSP, including any amendments to the PSP;

(k) proposing modifications to the PSP;

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

(m) attending meetings of the Committee;

(n) enhancing security awareness and vigilance by all staff;

(o) ensuring adequate security training has been provided to port employees and agents with regard to their security roles and responsibilities and maintenance of training records;

(p) ensuring that security equipment is appropriately operated, tested, calibrated and maintained;

(q) ensuring effective communication and cooperation between the port and members of the port security committee

(r) reporting all security incidents to the Committee; and

(s) overseeing the issue of copies of the PSP and maintaining a record of all authorised holders.

(t) ensuring compliance with the PSP and the implementation of complementary additional security measures as required by the Committee.

(u) The PSO shall initiate periodic internal audits or reviews of the PSP to ensure compliance with, and appropriateness of, existing security measures.

5 Maritime Security Committee

(1) The Maritime Security Committee is established for the purposes of maritime security of Niue.

(2) The Committee shall be appointed by Cabinet from time to time.

(3) The Chair of the Committee shall be appointed by Cabinet.

(4) The role of the Committee shall be to:

(a) coordinate the implementation of national maritime security measures in Niue ports and on Niue ships;

(b) provide a forum for the discussion of maritime security matters affecting port tenants/users and ships visiting the ports;

(c) provide a forum for communication between port tenants/users and shipowners on issues of security and procedures in place to meet threats, providing for normal situations and contingencies for periods of heightened tension and emergency situations;

(d) liaise, as considered appropriate, with external agencies to discuss security issues.

(e) provide advice on maritime security to the Committee, industry and the public; and

(f) advise the Committee of the need for additional security measures.

(5) The PSO shall ensure that a record of each meeting is kept and minutes are forwarded within one month of the meeting, either in written or electronic form, to all committee members.

(6) In the event of a security incident the PSO or shipowner must contact the Chair of the Committee who shall immediately convene a meeting of the Committee, along with other members as determined appropriate, who may set up a support team.

(7) The role of the support team under paragraph (6) is to:

(a) provide technical and operational advice and assistance to the police in relation to operational matters and resources available at the port;

(b) consult with the police, ensure the orderly conduct of other operations on the port not associated with the incident; and

(c) provide incident-related advice and information to their respective organisations and the Committee.

6 Security Levels

(1) Cabinet shall, when necessary, and with the recommendation of the Committee, set security levels and provide guidance for protection from security incidents.

(2) Higher security levels indicate greater likelihood of occurrence of a security incident.

(3) 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.

(4) Cabinet shall, when necessary, with the recommendation of the Committee, issue appropriate instructions and shall provide security related information to the ships and port facilities that may be affected.

(5) Additional security measures may be implemented either at the direction of the PSO or on the initiative of the Port Authority or the ship owner who shall give immediately advise the PSO.

(6) The Committee may delegate as appropriate certain duties under these Regulations other than:

(a) setting of the applicable security level;

(b) approving a PSA/PFSA/SSA and subsequent amendments to an approved assessment;

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

(d) approving a PSP/PFSP/SSP and subsequent amendments to an approved plan.

7 Declaration of Security

(1) A Declaration of Security must be completed in respect of a port or port facility when Cabinet deems it necessary or when a master deems it necessary.

(2) A Declaration of Security records the agreement reached between the ship and the port facility or with other ships with which it interfaces as to the respective security measures each will undertake in accordance with the provisions of their respective approved security plans.

(3) The need for a Declaration of Security may be indicated

(a) by the PSO pr PFSO,

(b) by the results of the PFSA or PSA,

(c) by the Maritime Administration of the flag state of a ship, or

(d) by the result of a SSA.

(4) A ship can request 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 that is not required to have and implement an approved port facility security plan; or

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

(5) If a ship, or a Maritime Administration on behalf of ships entitled to fly its flag, requests completion of a Declaration of Security, the PSO and SSO should acknowledge the request and discuss appropriate security measures.

(6) The Declaration of Security should be signed and dated by both the PSO and the master of SSO on behalf of the ship, as applicable, to indicate compliance with SOLAS chapter XI-2 and Part A of the ISPS Code and states its duration, the relevant security level and the relevant contact details.

(7) The Declaration of Security shall be completed in English and in the form prescribed in Schedule 8.

8 Port Security Plan

(1) The Committee shall in accordance with these Regulations conduct a PSA and produce a PSP, issued under the authority of Cabinet.

(2) The PSO shall prepare the Draft PSP and the Committee may approve its content prior to its circulation to those offices or persons approved by the Committee and shall approve all amendments prior to their being put into effect.

(3) The PSO may amend the PSP as necessary, subject to approval by the MSC.

(4) The completed PSP is classified "Confidential" and, while selected members of staff will need to be appraised of particular aspects of the Plan, it shall be protected from unauthorised access or disclosure.

(5) No part of the PSP may be reproduced or transmitted, in any form or by any means, without the written consent of the Committee.

9 Port Organisation and Responsibility

(1) All employees and agents of the Port Authority whose duties require them to implement security controls at the port or routinely access a restricted zone at the port must ensure that the protective security arrangements covered by the PSP are observed at all times.

(2) Any employee or agent on becoming aware of a:

(a) breach or suspected breach of security arrangements;

(b) any deficiency in the PSP; or

(c) who observes activities of a suspicious nature;

must report the matter immediately to the PSO.

(3) The Port Authority shall appoint a PSO who, with the authority of management, shall administer the day-to-day operations of the PSP at the port.

10 Port Facility Operators' Responsibility

(1) The Port Facility Operator shall, in co-operation with the Committee and in accordance with these Regulations, conduct a PFSA and produce a PFSP, issued under the authority of PSO.

(2) The PFSP shall be incorporated into the overall PSP where appropriate.

(3) The PSO shall review the draft PFSP and may approve its content prior to its circulation and shall approve all amendments prior to their being put into effect.

(4) The PSO may amend the PSP as necessary, subject to approval by the Committee.

(5) Port facility operators, lessees and tenants are responsible for:

(a) the security of their facilities and areas specifically allocated for their use;

(b) maintaining access control procedures as they apply to any of their facilities; and

(c) ensuring that any staff or other persons, such as contractors, who enter restricted zones or sterile areas do so only on current essential duties related to that area;

which could be effected through contractual arrangements.

(6) Port facility operators, lessees and tenants may be required, at short notice from the Port Authority or the PSO, to comply with security systems and/or procedure variations resulting from increases in maritime security threats.

(7) Security exercises, to test measures and response arrangements, shall be conducted by the PSO at a frequency agreed with the Committee.

(8) The object of the exercises is to not only test response arrangements to a simulated act of unlawful interference but to also:

(a) practice call out of all involved elements;

(b) test the adequacy of facilities;

(c) exercise members of the port security committee in the provision of effective support to police operational elements; and

(d) test the adequacy of appropriate contingency plans.

(9) The PSO and appropriate PSFOs will review each security exercise and submit a formal report to the Committee, within one month of the completion of the exercise.

11 Other Port Users

Any person who enters the port is required to comply with all regulatory provisions brought to their notice by any means including public notices, signs, announcements, publications or oral messages.

12 Shipping Organisation and Responsibility

(1) The Company shall ensure compliance with the SSP and for the implementation of complementary additional security measures as required by the Committee.

(2) The Company shall initiate periodic internal audits or reviews of the SSP to ensure compliance with, and appropriateness of, existing security measures.

(3) The Company shall appoint a CSO, who, with the authority of management, shall administer the overall operations of the SSP on all the Company's ships.

(4) The Company shall appoint a SSO for each ship, who, with the authority of management, shall administer the day-to-day operations of the SSP on each of the Company's ships.

(5) The duties and responsibilities of the CSO shall include:

(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 and regularly reviewed;

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

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

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

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

(g) enhancing security awareness and vigilance;

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

(i) ensuring effective communication and cooperation between the SSO and the relevant PFSOs and the PSO;

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

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

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

(m) authorising the issue of copies of the SSP and maintaining a record of all authorised holders.

(6) The duties and responsibilities of the SSO include:

(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 SSP;

(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 adequate training has been provided to shipboard personnel with regard to their security roles and responsibilities and maintenance of training records;

(h) reporting all security incidents;

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

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

(7) All employees and agents of the company, including crew, must ensure that the protective security arrangements covered by the SSP are observed at all times. Any employee or agent becoming aware of a:

(a) breach or suspected breach of security arrangements;

(b) any deficiency in the SSP; or

(c) who observes activities of a suspicious nature;

must report the matter immediately to the CSO or SSO as appropriate.

(8) Nothing in these Regulations removes from the master 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 any government as may be necessary.

13 Ship Security Plans

(1) Companies owning ships that are operating in Niue waters shall, in accordance with these Regulations and following discussion with the Committee, conduct a SSA and produce a SSP, issued under the authority of CSO.

(2) The PSO shall review the Draft SSP and the Committee may approve its content prior to its circulation to those offices and persons approved by the Committee and shall approve all amendments prior to their being put into effect.

(3) The CSO may amend the Plan as necessary, subject to approval by the Committee.

(4) The completed SSP is classified "Confidential" and, while Company staff and ship's crew will need to be apprised of particular aspects of the SSP, it shall be protected from unauthorised access or disclosure.

(5) No part of the SSP may be reproduced or transmitted, in any form or by any means, without the written consent of the CSO.

(6) The CSO may, at any time, review the SSP and in reviewing the SSP the CSO may have regard to:

(a) developments in relation to human and other resources used and procedures followed concerning ship security; and

(b) experience gained in relation to ship security by other ship operators.

(7) If the CSO is satisfied that:

(a) the approved SSP is no longer adequate for any one or more of the SSP purposes; or

(b) the effectiveness of the SSP for those purposes could be substantially improved:

the CSO should prepare and submit to the Committee for approval, proposals for any variation of the SSP considered necessary.

14 Contingency Procedures - Ports

(1) In the event of an employee or agent of the Port Authority or Port Facility Operator becoming aware of a significant act of unlawful interference or an unlawful threat, that person shall report the incident threat as soon as practicable to the PSO.

(2) Where the incident/threat directly impacts upon another organisation, or may impact upon one or other organisations, the PSO is to relay details of the incident threat to the organisation(s) concerned as soon as possible.

(3) The assessing and classifying of all threats, such as bomb or sabotage threats, against any of the port's amenities rests with the Committee, whereas assessing and classifying threats against a Port Facility Operator's amenities rests with the agency concerned.

(4) Threats are to be classified as either "GENUINE", in which case appropriate response procedures are to be instigated and followed, or "HOAX", in which case no further action (other than to report the incident to the police and the PSO) is required.

(5) Where the search of a building or facility (over which the Port Authority or Port Facility Operator has management control) is considered necessary, the threat shall be considered to remain genuine until the PSO advises that the threat has been reclassified as a hoax, or any suspicious object discovered during the search has been removed or declared safe.

(6) The PSO will report to the police details of significant breaches of security or threats impacting upon the operations of the Port Authority or Port Facility Operator involving violence.

(7) The PSO is to report, at the earliest opportunity, all security related incidents as well as actual or suspected acts of terrorism impacting upon the operations of the Port Authority or Port Facility Operator such as:

(a) discovery of weapons or disallowed items within the Port or Port Facility;
(b) unauthorised access to restricted areas;
(c) unauthorised access to a ship;
(d) bomb or sabotage threats:
(e) disruptive and/or abusive passengers or stevedores; and
(f) incidents that have attracted media attention

to the Committee.

(8) Contingency procedures shall be developed and maintained to provide for situations that could present a threat to the security of the Port or Port Facility.

(9) These procedures shall form part of the PSP or PFSP.

(10) Other types of emergencies that should be provided in the PSP or PFSP include:

(a) bomb search routine:
(b) evacuation procedures;
(c) security equipment failure; and
(d) action to be taken in respect of a major security incident at the port.

(11) Where it may not be possible to provide a full report within a reasonable time frame, due to the need to investigate certain aspects, a preliminary report shall be forwarded.

(12) The type of information that the PSO should include in any report to the Department is detailed at Schedule 6.

15 Contingency Procedures - Ships

(1) In the event of any person becoming aware of an act of unlawful interference on board a ship at sea or in port or an unlawful threat, that person shall report details of it as soon as practicable to the master, SSO or CSO as appropriate.

(2) Where the incident or threat directly impacts upon or may impact upon another organisation, the master or CSO must relay details of the incident/ threat to the other organisation as soon as possible.

(3) The duty of assessing and classifying of all threats, such as bomb or sabotage threats, against the ship or other facilities rests with the Company.

(4) Threats are to be classified as either "GENUINE", in which case appropriate response procedures are to be instigated and followed, or "HOAX", in which case no further action (other than to report the incident to the local police and the PSO) is required.

(5) Where a search is considered necessary, the threat shall be considered to remain genuine until the master or CSO advises that the threat has been reclassified as a hoax, or any suspicious object discovered during the search has been removed or declared safe.

(6) The master or CSO will report to the local police details of significant breaches of security or threats impacting upon the operations of the ship involving violence

(7) The master or CSO shall report, at the earliest opportunity, all incidents as well as actual or suspected acts of terrorism or other acts of unlawful interference that may affect the security of the ship, such as:

(a) discovery of weapons or disallowed items aboard the ship;
(b) unauthorised access to restricted areas;
(c) unauthorised access to the ship
(d) bomb or sabotage threats:
(e) disruptive and/ or abusive passengers; and
(f) incidents that have attracted media attention.

to the Committee.

(8) Contingency procedures shall be developed and maintained to provide for situations that could present a threat to the security of the ship and shall form part of the SSP.

(9) Other types of emergencies that should be provided in the SSP include:

(a) bomb search routine in port:
(b) bomb search routine at sea:
(c) repelling unsolicited boarders at sea;
(d) evacuation of the vessel;
(e) security equipment failure; and
(f) security procedures while in dry-dock or extended maintenance.

(10) Where it may not be possible to provide a full report within a reasonable time frame, due for example to the need to investigate certain aspects, a preliminary report shall be forwarded.

(11) The type of information that the SSO should include in any report to the CSO is detailed at Schedule 7. Upon receipt of the report the CSO shall forward a copy to the Department, which may contain supplementary information.

16 Security Training - Ports

(1) Responsibility for developing and maintaining the security awareness and training of the Ports Authority's employees and agents rests with the PSO and the Committee.

(2) The PSO and the Committee shall ensure that relevant employees and agents of the Ports Authority are provided with a basic level of training, the object of which is to establish a rudimentary level of security awareness. The minimum level of training shall include the following:

(a) port layout and organisations;
(b) the role of the Port Authority, the PSO, Police and other government agencies;
(c) basic port security procedures;
(d) access control;
(e) threat response; and
(f) other training specific to their duties.

(3) The Committee through the PSO shall ensure that employees and agents of the Ports Authority engaged in port security activities undertake more advanced training, which as a minimum shall include:

(a) principles of protective maritime security;
(b) legislation;
(c) IMO standards;
(d) law enforcement interface;
(e) passenger and baggage screening (where applicable);
(f) bomb threat assessment; and
(g) search and evacuation guidelines.

(4) The training modules offered shall be reviewed periodically, as shall the need for refresher training, with regard being given to developments in equipment used and procedures.

(5) The PSO shall ensure that records on the content, duration and dates of those training activities undertaken by employees and agents of the Ports Authority are retained for the previous five years.

(6) Port Facility Security Training is the responsibility of the Port Facility Operator who shall develop and maintain security awareness and training of its employees and agents, and shall follow as closely as possible the procedures required to be followed by the Port Authority for the ports in paragraphs (1) to (4).

17 Security Training – Ships

(1) The Company will ensure that all crew are provided with sufficient training to enable them to understand and carry out their security responsibilities.

(2) Training will consist of initial training in procedures and practices applicable to their position and, as appropriate, refresher training, which takes into account developments in relation to the equipment used and procedures followed relative to maritime security.

(3) The Company shall ensure that records of the content, duration and dates of those training activities undertaken by crewmembers are retained for the previous five years.

(4) Crew must be provided with current travel advice information prepared by the Office of External Affairs for those foreign ports they are to operate to or from and the potential impact that any special port security procedures in place may have.

18 Police powers

In addition to the powers and responsibilities set out in these regulations and in any other enactment in relation to the management and enforcement of maritime security, any constable shall have all the powers necessary for the proper enforcement of these regulations.

19 Offences

(1) Any person who contravenes or fails to comply with these Regulations, or the directions of an authorised person acting under these Regulations, commits an offence.

(2) Any person who possesses a disallowed item commits an offence.

(3) Any person who commits an act of unlawful interference commits an offence.

20 Penalties

A person who commits an offence under these Regulations is liable on conviction to a a fine not exceeding $10,000 or a term of imprisonment not exceeding 12 months.

21 Forms

Forms to be used are those set out in Schedules 1-8

SCHEDULE 1

Form of the International Ship Security Certificate

NIUE
INTERNATIONAL SHIP SECURITY CERTIFICATE

(Official seal) *(State)*

Certificate Number .....

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 Niue

by the Minister of National Security

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 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 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 Convention and part A of the ISPS Code;

3 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 Alofi by the Secretary to Government _____ (signature)

Issued on the .....day of..... 20..... _____(Seal or Stamp)

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 Convention and part A of the ISPS Code.

Intermediate verification -

At Alofi on the .....day of..... 20.....

Signed .....
(Secretary to Government)

(Seal or Stamp of the authority, as appropriate)

ENDORSEMENT FOR ADDITIONAL VERIFICATIONS*

Additional verification -

At Alofi on the .....day of..... 20.....

Signed .....
(Signature of Secretary to Government)

(Seal or Stamp of the authority, as appropriate)

Additional verification -

At Alofi on the .....day of..... 20.....

Signed .....
(Signature of Secretary to Government)

(Seal or Stamp of the authority, as appropriate)

Additional verification -

At Alofi on the .....day of..... 20.....

Signed .....
(Signature of Secretary to Government)

(Seal or Stamp of the authority, as appropriate)

* This part of the certificate shall be adapted by the Maritime Administration/Port Authority to indicate whether it has established additional verifications as provided for in section 19.1.1.4.

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 Convention and part A of the ISPS Code.

Additional verification -

At Alofi on the .....day of..... 20.....

Signed .....
(Signature of Secretary to Government)

(Seal or Stamp of the authority, as appropriate)

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 the ..... day of ..... 20.....

Signed .....
(Signature of Secretary to Government)
At Alofi on the .....day of..... 20.....

(Seal or Stamp of the authority, as appropriate)

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 the ..... day of ..... 20.....

Signed .....
(Signature of Secretary to Government)
At Alofi on the .....day of..... 20.....

(Seal or Stamp of the authority, as appropriate)

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* of part A of the ISPS Code, be accepted as valid until the ..... day of ..... 20.....

Signed .....
(Signature of Secretary to Government)
At Alofi on the .....day of..... 20.....

(Seal or Stamp of the authority, as appropriate)

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 the ..... day of ..... 20.....

Signed .....
(Signature of Secretary to Government)
At Alofi on the .....day of..... 20.....

(Seal or Stamp of the authority, as appropriate)

---

* Delete as appropriate.

** 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.

SCHEDULE 2

Form of the Interim International Ship Security Certificate

NIUE

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal) *(State)*

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 Niue

by the Minister of National Security

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.

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 Alofi by the Secretary to Government _____(signature)

Issued on the .....day of ..... 20..... _____(Seal or Stamp)

* Delete as appropriate

SCHEDULE 3

Form of the International Ship Security Certificate

NIUE

STATEMENT OF COMPLIANCE OF A PORT OR PORT FACILITY

(Official seal) *(State)*

Certificate Number .....

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 Niue

by the Minister of National Security

Name of Facility: .....

Address: .....

Telephone: ..... Fax: .....

..... Chief Executive Officer Email .....

Port Facility Security Officer and Contact Details

..... Harbour Master Email .....

Telephone: ..... Fax: ..... Mobile .....

THIS IS TO CERTIFY THAT the requirements of the provisions of SOLAS Chapter XI-2 and part A of the ISPS Code have been complied with.

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

This Certificate is valid until .....

Issued at Alofi by the Secretary to Government .....(signature)

Issued on the .....day of ..... 20..... .....(Seal or Stamp)

SCHEDULE 4

GUIDELINES FOR THE DEVELOPMENT OF PORT AND PORT FACILITY SECURITY PLANS

The following is for the guidance of ship owners and operators of ships to whom these Regulations apply.

1. Facility Access Control Measures

(1) Peripheral protection of the restricted zone is provided by intrusion protection and detection equipment. It is normally achieved by installing security barriers (fencing), which can be complemented by installing peripheral or close intrusion detection equipment and/or intrusion display equipment. Openings in security barriers should be kept to a minimum and secured when not in use. Security barriers should accomplish the following:

(a) define the area to be protected;

(b) create a physical and psychological deterrent to persons attempting or contemplating unauthorised entry;

(c) delay intrusion, enabling operating personnel and security guards to detect and apprehend intruders; and

(d) provide designated and readily identifiable places for entry of personnel and vehicles into areas where access is controlled.

(2) Where feasible, buildings and other suitable permanent obstacles should be used as part of the physical barrier, provided that access through the buildings used is controlled. If buildings are used as part of the security barrier, they should be inspected to ensure that windows, roofs, ventilation openings, etc, do not provide for unauthorised access, with consideration being given to the fitting of bars, grills or screens.

2. –Access Control Measures - Staff

Only those employees/ agents who have a legitimate need to access the facility operator's restricted zone shall enter the area. Other staff members will need to justify a need for access to the PFSO.

3. –Access Control Measures – Service Providers & Visitors

(1) Where a service provider, such as a maintenance contractor or a ship's providor, requires access to a restricted zone their need to access the area shall be verified with the requesting organisation.

(2) Where that need can be established the person(s) may be authorised to enter the restricted zone. However, where the need cannot be established the person is to be denied entry and the matter bought to the attention of the PFSO, who in turn may consider it appropriate to inform the police.

(3) Visitors with a legitimate requirement for access to a restricted zone shall remain under supervision by their sponsor at all times during the visit.

(4) The identity of each non-employee/ non-agent provided access to the restricted zone is to be recorded, for each visit, in a visitor's register. The minimum detail to be

recorded shall comprise their name, organisation represented, arrival time, departure time, who sponsored their visit. The register is to also show the signature of the person authorising their access to the restricted zone.

(5) Records of those persons authorised to access the restricted zone will be retained by the PFSO for a period of twelve months.

4. Access Control Systems

(1) Where access points into the restricted zone are key-controlled a restricted key system is to be used.

(2) Keys will only be issued, by the PFSO, to authorised persons (e.g. staff and regular contractors) who have a valid reason to access to the restricted zone in the course of their duties.

(3) A key register will be maintained detailing to whom specific keys have been issued as well as the date of issue and return (where appropriate). Recipients are to sign the register for each key issued.

(4) Change of coding should be considered where control of any key is lost. Coding must be changed when 5% or more of the keys to any particular lock cannot be accounted for.

(5) Where an electronic access control system is fitted access rights will only be provided, by the PFSO, to authorised persons who have a valid reason to access the restricted zone in the course of their duties.

(6) A register of those with access rights will be maintained detailing to whom specific rights have been provided as well as the date granted, date withdrawn (where appropriate), the areas into which the holder has access and any prohibitions that may apply (e.g. access limited to certain hours).

(7) The PFSO shall audit bi-annually the manual and electronic systems registers and ensure that any deficiencies are rectified within one month of the audit.

(8) Keys and access cards, or changes to access cards, will only be effected where the applicant has requested the issue change in writing and the request is approved by their supervisor/manager.

5. –Electronic Surveillance

Enhanced surveillance over specific facilities/ installations or specific areas may be determined essential to guard against a perceived threat and could involve the use of the following types of equipment: CCTV or intruder detection systems.

SCHEDULE 5

GUIDELINES FOR THE DEVELOPMENT OF SHIP SECURITY PLANS

The following is for the guidance of ship owners and operators of ships to whom these Regulations apply.

1. – Restricted Areas

(1) Ship Security Plans shall show the following:

(a) the location of restricted areas (e.g. bridge, engine room, steering gear compartments, officers' cabins and crew accommodation);

(b) the location and function of actual or potential access points (e.g. ladders, gangways, scuttles, mooring lines and cranes); and

(c) spaces with security and surveillance equipment, cargo spaces, spaces containing ship's stores or hazardous substances.

(2) A sign advising those areas that are restricted to authorised personnel shall be prominently displayed on those doors providing initial access to each restricted area. These signs will be maintained in good condition and be clearly legible.

2. – Access Control

(1) It is Company policy that all entrances to the ship are closed unless the master decides there are operational reasons to have one or more of these open. All open access points must be protected to the same standard.

(2) The master should consider all operational and potential security impacts when deciding how many gangways are rigged at each port. This decision should consider the Security Level and allocation of crew for security surveillance activities.

(3) While in port no shell door will be opened under any circumstances without the express permission of the Officer on Watch. At sea, no shell door will be opened without permission of the master. Where a shell door is to remain open a member of crew shall be placed on guard duty to prohibit unauthorised entry.

(4) All doors allowing access to restricted areas shall be secured (where practicable), controlled and regularly inspected. The intention is to establish secure areas that unauthorised persons will find difficult to penetrate while being cognisant of other requirements, such as the need to provide for emergency egress.

(5) Where an access point is via a gangway, ramp or ladder and is used at night, the area surrounding that access point shall be adequately illuminated.

(6) All persons, other than crew, proposing to board the ship will need to have a justifiable reason to access the ship prior to entry being authorised.

(7) Crewmembers shall challenge all persons, other than authorised crew, in a restricted area should the person not be displaying an appropriate form of company identification or the person is not under escort by another member of the crew.

(8) The identity of those persons authorised the access a restricted area shall be recorded, for each visit, in a visitor's register. The minimum detail to be recorded shall comprise their name, organisation represented, arrival time, departure time, who

sponsored their visit. The register is to also show the signature of the person authorising their access to the restricted area.

(9) Records of those persons authorised to access the restricted area will be retained by the SSO for a period of twelve months.

(10) Visitors, other than service providers such as an accredited maintenance contractor or ship's provider, with a legitimate requirement to access a restricted area shall remain under supervision of the SSO, or someone nominated by the SSO, while within a restricted area.

3. – Access Control Systems

(1) Where access points into the restricted area are key-controlled a restricted key system is to be used.

(2) Keys will only be issued, by the SSO, to crewmembers who have a valid reason to access to the restricted area in the course of their duties.

(3) A key register will be maintained detailing to whom specific keys have been issued as well as the date of issue and date of return (where appropriate). Recipients are to sign the register for each key issued.

(4) Where an electronic access control system is fitted access rights will only be provided, by the SSO, to crewmembers who have a valid reason to access the restricted area in the course of their duties.

(5) A register of those with access rights will be maintained detailing to whom specific rights have been provided as well as the date granted, date withdrawn (where appropriate), the areas into which the holder has access and any prohibitions that may apply (e.g. access limited to certain hours).

(6) The SSO shall audit bi-annually the manual and electronic systems registers and ensure that any deficiencies are rectified within an agreed timeframe, which shall be as soon as practicable.

(7) Keys and access cards, or changes to access cards, will only be effected where the applicant has requested the issue/ change in writing and the request is approved by their supervisor/ manager.

4. – Restricted Area Breach

(1) In the event of a detected breach of security in a restricted area the SSO will arrange for the incident to be investigated and a sweep of the affected area will be conducted. The purpose of the sweep will be to determine the method of unauthorised access, check for evidence of tampering to commodities, etc and locate any suspicious objects prior to the recommencement of operations in the area.

(2) In each case those security measures and procedures breached will be re-evaluated with the view to remedying any inherent or perceived weaknesses.

5. – Screening of Passengers & their Baggage

(1) On each occasion that a prospective passenger presents for boarding, the company will ensure that:

(a) the passenger has valid travel documentation;

(b) baggage is only accepted from ticketed passengers;

(c) baggage is only accepted at a designated check-in point;

(d) a tag displaying the relevant passenger's name and the total number of items checked in, at that time, by that passenger is securely attached to each item of baggage accepted for carriage; and

(e) prior to the baggage being loaded, baggage accepted for carriage will not be accessible by a person other than a person authorised by the port facility operator or company, the owner of the item (once they have been screened), and those involved in loading the item aboard the ship.

(2) The company will ensure that all passengers and their possessions are, prior to their entering any sterile area used for departing passengers, subject to screening procedures by an approved screener unless specifically exempted pursuant to the Department's maritime security regulations.

(3) The company will ensure that the sterile area into which the screened passengers pass is an area properly secured against unauthorised entry and exit.

(4) Where there is no sterile area the company will ensure that all passengers and their possessions are, prior to their being provided access to the ship, subject to screening procedures by an approved screener unless specifically exempted pursuant to the Department's maritime security regulations.

(5) The company will ensure that passengers, or intending passengers, of the ship who have been screened do not make physical contact with persons, vehicles or goods that have not been screened or cleared for purposes of maritime security unless the persons, vehicles or goods are specifically exempted pursuant to the Department's maritime security regulations.

(6) When a weapon or other disallowed item is detected during the screening process it must be surrendered if the passenger wishes to travel. Surrendered weapons or disallowed items may be carried aboard the ship in a secure manner and returned to the passenger at his or her destination point.

(7) An approved screener must not screen a passenger, other than by a physical search, should the passenger elect to be screened by means of a physical search.

(8) The tag attached to unaccompanied baggage is to be checked prior to the baggage being loaded aboard the ship. Any unaccompanied baggage that is not tagged shall not be loaded until the legitimacy of the baggage can be verified by the SSO.

(9) Strict control shall be exercised over tags used to identify authorised baggage to limit the likelihood of rogue bags being introduced into the baggage stream.

(10) When in an overseas port, prior to allowing any passengers and their baggage aboard, the SSO/ CSO will need to be satisfied that security measures, in relation to the handling of passengers and their baggage, are consistent with the ISPS Code.

6- . . .

7 – Screening of Ship's Crew & Visitors

(1) All crew, guests of crew and service providers (e.g. maintenance contractors and providors), and goods in their possession will be screened should they board the ship via an active passenger screening point, unless specifically exempted pursuant to the Department's maritime security regulations.

(2) Crew, guests of crew and service providers who enter the ship via an alternate means, separate from the sterile area, need not be subject to screening.

8 – Crew Baggage

(1) Until baggage is checked in or taken aboard the ship, crewmembers are at all times responsible for the security integrity of their baggage.

(2) Where crew baggage is consolidated prior to check-in or being stowed aboard the ship, the baggage is to be kept under constant surveillance by a crewmember or other authorised person.

9 – Cargo Handling

(1) Cargo accepted for export (from Niue) shall be in accordance with Niue Customs Service requirements. This recognises that all goods for export come under Customs control and also recognises the established preventive security measures, both physical and procedural, that Niue Customs Service has in place with regard to those goods.

(2) Prior to loading packaged and containerised export or domestic cargo the cargo is to undergo a cursory inspection to ensure that there are no obvious signs of tampering.

(3) Any obvious signs of tampering or damage must be referred to the SSO and the cargo handler. If a satisfactory explanation cannot be established the cargo shall not to be accepted. Should there be a satisfactory reason for the loss of integrity then the damage shall be made good before acceptance.

(4) The SSO shall contact the local police or the Australian Customs Service in suspicious circumstances.

(5) For both export and domestic cargo, where a cargo handler (e.g. stevedore) who is challenged by a crewmember is unable to produce appropriate identification then the goods shall not be accepted.

(6) When the ship is in an overseas port, prior to accepting goods the SSO/ CSO will need to be satisfied that security measures, in relation to the handling of cargo, are consistent with the ISPS Code.

10 – Ship's Stores

(7) All stores are to be individually accepted by a member of the ship's crew, with evidence that they were ordered made available prior to their being loaded aboard the ship.

(8) Prior to acceptance, the goods are to undergo a cursory inspection by crew to ensure that there are no obvious signs of tampering

(9) Any signs of obvious tampering or damage must be referred to the SSO and the port facility operator/ transporter. If a satisfactory explanation cannot be established the goods are not to be accepted. Should there be a satisfactory reason for the loss of integrity then the damage shall be made good before acceptance.

(10) For passenger ships, and where X-ray equipment is in use, the stores should (where possible) be "broken down" and screened via the use of the X-ray equipment, which is to be operated by an approved screener.

(11) For passenger ships, where X-ray equipment is not available, or the item is too large to fit through the frame of the X-ray equipment, those stores are to be subject to a detailed physical search by approved screeners.

(12) In a limited number of cases those screening the stores may be satisfied that the goods do not contain a weapon or disallowed item, based on other considerations, such as the surrounding circumstances of the arrival of the goods at the ship. For example, the goods are transported within a pre-existing and secure scheme known to the screener.

THREAT/INCIDENT REPORT

PORT OR PORT FACILITY

SCHEDULE 6

General information

Name of Port/ Facility: .....

Person providing Report: .....

Date : ..... Time: ..... Location: .....

Type of occurrence (e.g. bomb/ sabotage threat, unauthorised entry, suspect device, extortion, etc)

.....

Description of threat/ incident

.....

.....

.....

.....

.....

.....

.....

Alleged offender(s)

Name: ..... Nationality: .....

Name: ..... Nationality: .....

Name: ..... Nationality: .....

Name: ..... Nationality: .....

Nature and severity of any injuries sustained by others

Name: ..... link to port: ..... Injury: .....

Name: ..... link to port: ..... Injury: .....

Name: ..... link to port: ..... Injury: .....

Name: ..... link to port: ..... Injury: .....

Circumstances surrounding device(s) used

Type of Device(s): .....

.....

Method of introduction (e.g. passenger, baggage, cargo, stores, etc): .....

.....

.....

Security measures circumvented: .....

.....

.....

Proposed measures and procedures to prevent recurrence of a similar event?

.....

.....

.....

Other pertinent details

.....

.....

.....

.....

.....

.....

.....

.....

.....

Reporting Officer

Signature: ..... Name (printed): .....

Designation: ..... Date: .....

Upon receipt of this report the PSO shall forward a copy to the Department.

THREAT/INCIDENT REPORT

SHIP

SCHEDULE 7

General information

Name of Ship: .....

Person providing Report: .....

Date : ..... Time: ..... Location: .....

Type of occurrence (e.g. bomb sabotage threat, unauthorised entry, passenger incident, suspect device, etc)

.....

Description of threat/ incident

.....

.....

.....

.....

.....

.....

.....

Alleged offender(s)

No. Passengers: ..... No. Crew: ..... Other: .....

Name: ..... Nationality: ..... Embarked: .....

Name: ..... Nationality: ..... Embarked: .....

Name: ..... Nationality: ..... Embarked: .....

Nature and severity of any injuries sustained by passengers, crew or others

Name: ..... Crew/ Pass/ Other: ..... Injury: .....

Name: ..... Crew/ Pass/ Other: ..... Injury: .....

Name: ..... Crew/ Pass/ Other: ..... Injury: .....

Name: ..... Crew/ Pass/ Other: ..... Injury: .....

Circumstances surrounding device(s) used

Type of Device(s): .....

.....

Method of introduction (e.g. passenger, baggage, cargo, stores, etc): .....

.....

.....

Security measures circumvented: .....

.....

.....

Proposed measures and procedures to prevent recurrence of a similar event?

.....

.....

.....

Other pertinent details

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Reporting Officer

Signature: ..... Name (printed): .....

Designation: ..... Date: .....

Upon receipt of this report the CSO shall forward a copy to the Department.

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.

Activity	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:	
	The port facility	The ship
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized 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		

* 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.