SHIP SECURITY PLAN

Version 1.0
August 2003

W. G. JACKSON

Grand Valley State

{Note: Because this is a generic plan rather than a ship-specific plan, it is not marked as sensitive information. Typically, ship security plans should be plainly marked to warn personnel having access to the plan that it needs to be protected and should not be released. Also, companies will need to coordinate with their flag administration and port facility security officers to determine what specific security information protection measures apply.}

[SHIP NAME] Security Plan

Revision Record

Revision Number	Date of Revision	Name/Rank of Person Making the Revision	Signature

INDEX

SECTION 1

INTRODUCTION AND PURPOSE

1.1 Purpose and Regulatory Basis

The purpose of this Ship Security Plan (SSP) is to contribute to the prevention of illegal acts against the ship and its crew. It has been prepared in accordance with:

- The ABS *Ship Security Guide*
- Chapter XI-2 of SOLAS
- The International Ship and Port Security (ISPS) Code, Part A
- The International Ship and Port Security (ISPS) Code, Part B, paragraphs 8.1 through 13.8
- United States Coast Guard (USCG) Regulation 33 CFR Subchapter H Part 104
- ***{Note: Here the plan should list any specific flag state or port state regulatory requirements that the ship plan is designed to meet and provide the contact points and reporting procedures to them.}***

1.2 Plan Documentation and Control

Authorized copies of this SSP must be controlled so all authorized holders of the plan have the current revision. The Ship Security Officer (SSO) is responsible for issuing revisions to this plan, after the revisions have been approved by the Master and the Company Security Officer (CSO). Significant changes to this plan must also be approved prior to implementation by the flag administration or a Recognized Security Organization (RSO) approved by the flag administration.

1.3 Periodic Review Procedures

This plan must be reviewed annually by the SSO, based in part on the results of the annual security assessment performed by the CSO. If revisions are required, they will be drafted by the SSO for review and approval as specified above.

1.4 Plan Security and Control

Distribution of this SSP must be controlled so that it is restricted to personnel that have a need to know for purposes of implementing or assessing the security plan for this ship. The requirement to protect this information must be covered in security training sessions provided for company personnel. Also, all copies of this plan should be marked as specified by the company security program. All transmittals of a copy of the information in this plan should include a warning that the information is sensitive and must be protected.

{Note: Because this plan is a generic one rather than a ship specific plan, it is not marked as security sensitive information. Typically ship security plans should be plainly marked to warn personnel having access to the plan that it needs to be protected and should not be released. Procedures shall be addressed on how the ship security plan is protected from unauthorized access or disclosure. The company should address whether the ship security plan is kept in an electronic format and whether it is protected by procedures aimed at preventing unauthorized deletion, destruction, or amendment. Also, companies will need to coordinate with their flag administration and port authorities to determine what specific security information protection measures apply.}

{Note: This plan is not organized in the specific format detailed in section §104.405 (a) of the USCG regulation 33 CFR Subchapter H. Table 1 indexes the USCG sections to the corresponding sections of this plan and Table 2 references the corresponding USCG terminology to the corresponding terminology in this plan.}

TABLE 1

CROSS REFERENCE OF USCG REGULATION 33 CFR SUBCHAPTER H 104.405 (a) TO SHIP SECURITY PLAN

USCG Section	SSP Section
(1) Security organization of the vessel	Section 4
(2) Personnel training	Section 4.2.1
(3) Drills and exercises	Section 4.2.2
(4) Records and documentation	Section 4.3
(5) Response to change in SECURITY Level	Section 14
(6) Procedures for interfacing with facilities and other vessels	Section 4.5
(7) Declaration of Security (DoS)	Section 5
(8) Communications	Section 12; Section 14 Table 2
(9) Security systems and equipment maintenance	Section 11
(10) Security measures for access control	Section 6; Section 14 Table 4
(11) Security measures for restricted areas	Section 7; Section 14 Table 3
(12) Security measures for handling cargo	Section 8; Section 14 Table 7
(13) Security measures for delivery of vessel stores and bunkers	Section 9; Section 14 Table 7
(14) Security measures for monitoring	Section 11; Section 14 Table 5
(15) Security incident procedures	Section 13
(16) Audits and Vessel Security Plan (VSP) amendments	Section 4.4
(17) Vessel Security Assessment (VSA) Report	Section 19

TABLE 1

CROSS REFERENCE OF USCG REGULATION 33 CFR SUBCHAPTER H PART 104 TERMINOLOGY TO THIS SHIP SECURITY PLAN TERMINOLOGY

USCG Terminology	SSP Terminology
Vessel Security Officer (VSO)	Ship Security Officer (SSO)
Vessel Security Plan (VSP)	Ship Security Plan (SSP)
Vessel Security Assessment (VSA)	Ship Security Assessment (SSA)
Captain of the Port (COTP)	Port Authorities
Facility	Port Facility
Facility Security Officer (FSO)	Port Facility Security Officer (PFSO)
Vessel	Ship

SECTION 2

DEFINITIONS

Calling Port: Port where a ship moors (or anchors) and crew are allowed to leave the ship to visit the port. Crew baggage and ship stores will not normally be loaded or off-loaded at calling ports.

Company Security Officer (CSO): The company official from the ship operator who will be responsible for developing, maintaining and enforcing the company security policies as set out in this document.

Disembark: Refers to any time that the crew leave the ship, be it a port call or final destination.

Embark: Refers to any time that crew board the ship, be it a port of call or initial boarding of the ship.

Operator: The person, company, or government agency, or the representative of a company or government agency, which maintains operational control over a terminal that the ship will visit.

Port Facility Security Officer (PFSO): Person designated as responsible for the development, implementation, revision, and maintenance of the port facility security plan and for liaison with the port authorities and Ship Security Officers and Company Security Officers.

Ship Security Officer (SSO): The specific individual onboard the ship who is designated by the Company. The SSO reports to the Master for the overall management and oversight of all shipboard security policies, programs and procedures. The SSO is identified by name and position on the ships crew list and in the advance notice of arrival.

Terminal: Any structure used for the assembly, processing, embarking, or disembarking of cargo for the ship. It includes piers, wharves, and similar structures to which a ship may be secured; land and water under or in immediate proximity to these structures; buildings on or contiguous to these structures; and equipment and materials on or in these structures.

Unlawful Act: An act that is a violation under the laws of the states where the ship is located, or under the laws of the country in which the ship is registered.

Voyage: The ship's entire course of travel, from the first port at which the ship loads cargo until its return to that port or another port where the majority of the cargo is offloaded and the ship terminates that voyage.

Security Levels:

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 transportation 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 transportation security incident is probable or imminent, although it may not be possible to identify the specific target.

SECTION 3

CONTACT INFORMATION AND SHIP DETAILS

3.1 CONTACT INFORMATION

a. Company Headquarters

Company Name:

Address:

Phone Number:

Fax Number:

Other:

b. Company Security Officer (CSO)

Name:

Phone Number:

Pager Number:

Other:

c. Ship Security Officer (SSO)

Name:

Phone Number:

Pager Number:

Other:

3.2 SHIP DETAILS

{List specific ship information in this section. If specific ship information is provided in another document, a reference to that document may be listed here instead of ship details.}

SECTION 4

SECURITY POLICIES

4.1 STRUCTURE OF SECURITY

The following section describes the structure of security including the duties of the Master, CSO, and SSO.

{Note: The company should address the organizational structure of security for the ship.}

4.1.1 THE MASTER

Nothing in this SSP is intended to permit the Master to be constrained by the Company, the ship owner or operator, 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 authorized by the cognizant government authority—or their effects, and refusal to load cargo, including containers or other closed cargo transport units.

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 will give precedence to measures intended to maintain the safety of the ship, and take such temporary security measures as seem best under all circumstances. In such cases:

1. The Master will, as soon as practicable, inform the relevant maritime authority of the flag Administration. If the ship is in port, intends to enter a port the relevant authorities having jurisdiction over that port must also be informed. If the ship is interfacing, or intends to interface with another ship, port facility, or terminal, the security officer of that ship, port facility, or terminal must also be notified.
2. The temporary security measures will, to the highest possible degree, be commensurate with the prevailing Security Level;

4.1.2 COMPANY SECURITY OFFICER (CSO)

a. The Company Security Officer (CSO) is responsible for all aspects of security.

b. The duties of the CSO are to include:

1. Advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information.
2. Ensuring that ship security assessments are carried out.
3. Ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan.
4. Ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship.
5. Arranging for internal audits and reviews of security activities, including inspections by government authorities.
6. Arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security Organization.
7. Ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with.

8. Enhancing security awareness and vigilance.
9. Ensuring adequate training for personnel responsible for the security of the ship.
10. Ensuring effective communication and co-operation between the Ship Security Officer and the relevant port facility security officers.
11. Ensuring consistency between security requirements and safety requirements.
12. Ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately.
13. Ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.
14. Ensure security measures give particular consideration to the convenience, comfort, and personal privacy of ship personnel and their ability to maintain their effectiveness over long periods.

c. The CSO has direct access to the highest level of management and is responsible for the development, implementation, and efficiency of [**COMPANY**] security policies.

d. ***{Note: List any other duties of the CSO provided he or she is able to perform the before mentioned required responsibilities.}***

4.1.3 SHIP SECURITY OFFICER (SSO)

The Ship Security Officer (SSO) reports to the Master for the overall management and oversight of all shipboard security policies, programs and procedures. His responsibilities include, but are not limited to:

a. Performing regular security inspections of the ship to ensure that appropriate security measures are maintained.

b. Implementing and maintaining the ship security plan (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 port facility security officers.

d. Proposing modifications to the ship security plan to correct deficiencies and satisfy the security requirement of the ship.

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. Ensuring security awareness and vigilance onboard the ship and within terminals.

g. Ensuring that adequate training has been provided for all personnel responsible for security.

h. Reporting all occurrences or suspected occurrences of unlawful acts concerning any port to the relevant Port Facility Security Officer (PFSO) and ensuring that the report is forwarded, with information to the Master, to the CSO, and where necessary, to the ship's flag state's designated authority.

i. Reporting all occurrences or suspected occurrences of unlawful acts committed onboard the ship, to the Master, and the CSO.

j. Coordinating the implementation of the ship security plan with the CSO and the designated PFSO.

k. Ensuring that security equipment is properly operated, tested, calibrated, and maintained

l. The implementation of [COMPANY] procedures pertaining to security, as directed by the Master.

m. Implementing policies and procedures regarding security duties assigned to ship personnel.

n. Managing shipboard security staff.

o. Establishing close liaison with all law enforcement agencies at all ports of call.

p. Completing the Declaration of Security on behalf of the ship

{Note: List any other duties of the SSO provided he or she is able to perform the before mentioned required responsibilities.}

4.1.4 COMPANY OR SHIP PERSONNEL WITH SECURITY DUTIES

Company and ship personnel responsible for security duties have knowledge, through training or equivalent job experience, in the following, as appropriate:

a. Knowledge of current security threats and patterns;

b. Recognition and detection of dangerous substances and devices;

c. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

d. Techniques used to circumvent security measures;

e. Crowd management and control techniques;

f. Security related communications;

g. Knowledge of emergency procedures and contingency plans;

h. Operation of security equipment and systems;

i. Testing and calibration of security equipment and systems, and their maintenance while at sea;

j. Inspection, control, and monitoring techniques;

k. Relevant provisions of the Ship Security Plan (SSP)

l. Methods of physical screening of persons, personal effects, baggage, cargo, and ship stores; and

m. The meaning and the consequential requirements of the different Security Levels.

{Note: The company should address the duties of other shipboard personnel with security responsibilities as well as security aspects of the duties of other shipboard personnel at each security level.}

4.2 SECURITY POLICIES

The following section describes security policies established on the ship.

4.2.1 TRAINING

The SSO is responsible for ensuring that security training is conducted. He is responsible for ensuring all other ship personnel, including contractors, whether part-time, fulltime, temporary, or permanent, have knowledge of, through training or equivalent job experience in the following:

a. Relevant provisions of the SSP;

b. The meaning and the consequential requirements of the different Security Levels, including emergency procedures and contingency plans;

c. Recognition and detection of dangerous substances and devices;

d. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

e. Techniques used to circumvent security measures.

4.2.2 DRILLS AND EXERCISES

Drills and exercises are used to test the proficiency of ship personnel in assigned security duties at all Security Levels and ensure effective implementation of the SSP.

a. Drills

1. The SSO ensures that a security drill is conducted at least every 3 months. Security drills and non-security drills are held in conjunction where appropriate. Under the circumstance that the ship is out of service due to repairs or seasonal suspension of operation, the 3-month time frame is extended and a drill is conducted within one week of the ship's reactivation.

2. Drills test individual elements of the SSP, including response to security threats and incidents. Drills take into account the types of operations of the ship, ship personnel changes, and other relevant circumstances.

   {Note: The company should provide a list of example drills such as unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.}

3. When the ship is moored at a port facility on the date the port facility has planned to conduct any drills, the ship may choose to participate, while not required to, in the port facility's scheduled drill.

4. Drills are conducted within one week whenever the percentage of ship personnel with no prior participation in a ship security drill on that ship exceeds 25 percent.

b. Exercises.

1. Exercises are conducted at least once each calendar year, with no more than 18 months between exercises.

2. Exercises are either:

   i. Full scale or live;

   ii. Tabletop simulation or seminar;

   iii. Combined with other appropriate exercises; or

   iv. A combination of the elements of the above-mentioned exercises.

3. Exercises are ship-specific or part of a cooperative exercise program to exercise applicable facility and ship security plans or comprehensive port exercises.

4. Each exercise tests communication and notification procedures, and elements of coordination, resource availability, and response.

5. Exercises are a full test of the security program and include the substantial and active participation of relevant company and ship security personnel, and include facility security personnel and government authorities depending on the scope and the nature of the exercises.

{Note: The following tables provide a format for outlining the training, drills, and exercises that are implemented as part of the ship security program.}

Security Training Schedule			
Item	**Involving**	**Frequency**	**Comments**
Training Sessions			
Initial Security Awareness Training	Entire ship crew	When initially assigned to ship	
Refresher Security Briefing	Entire Ship Crew	Annually	
Security Plan Training	Selected crew members	When assigned Also when the plan is revised	Should include all personnel who have a role in implementing any action in the security plan
Ship Security Officer Training	All personnel that will assume the role of SSO	When assigned	Should cover regulatory basis for and development / maintenance of security plans
Security Staff Training	All personnel whose full time job is a security function	When assigned	Can be modified based on the law enforcement / security experience of the candidate
Security equipment	Personnel assigned to use the equipment	Prior to assignment	May be adequate implement manufacturer provided procedures and training
{Note: This table should be completed for all training activities. These entries serve as examples only.}			

Drills/Exercises Schedule			
Bomb Threat/Bomb Search Drill	Bomb search personnel	Annually	Should also be covered in training when individuals are assigned
Watchstanding in Security Level 3 Environment	All security watch personnel	Annually	
Contraband Baggage Introduction (e.g. mock weapon)	Baggage screeners	Periodically based on equipment and procedures	Exercise should be conducted without prior knowledge of screeners
{Note: This table should be completed for all drills and exercises. These entries serve as examples only.}			

4.3 RECORDS AND DOCUMENTATION

a. A Security Daily Occurrence Log is maintained by the SSO and is made available to the Master as required.

b. Upon completion, all Daily Occurrence Logs are to be retained onboard for one year, after which they are to be forwarded to the CSO.

c. Copies of serious incidents noted in the log are to be transmitted to the CSO via e-mail or fax within 24 hours of the incident occurring.

d. The SSO keeps records of the following activities for at least 2 years and makes them available upon request. These records may be kept in electronic format, and if so must be protected against unauthorized deletion, destruction, or amendment and must be protected from unauthorized access or disclosure:

1. Training - For each security training session, the date of each session, duration of session, a description of the training, and a list of attendees;

2. Drills and exercises - For each drill or exercise, the date held, description of drill or exercise, list of participants; and any best practices or lessons learned which may improve the SSP;

3. Incidents and breaches of security - Date and time of occurrence, location within the port, location within the ship, description of incident or breaches, to whom it was reported, and description of the response;

4. Changes in Security Levels - Date and time of notification received, and time of compliance with additional requirements;

5. Maintenance, calibration, and testing of security equipment - For each occurrence of maintenance, calibration, and testing, the date and time, and the specific security equipment involved;

6. Security threats - Date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported, and description of the response;

7. Declaration of Security (DoS) - Manned ships must keep on board a copy of the last 10 DoSs and a copy of each continuing DoS for at least 90 days after the end of its effective period; and

8. Annual audit of the SSP - For each annual audit, a letter certified by the SSO stating the date the audit was completed.

4.4 SECURITY AUDIT

a. *Audits.*

1. The CSO ensures an audit of the SSP is performed annually, beginning no later than one year from the initial date of approval and attach a letter to the SSP certifying that the SSP meets the applicable requirements.

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

3. Auditing the SSP as a result of modifications to the ship may be limited to those sections of the SSP affected by the ship modifications.

4. Unless impracticable due to the size and nature of the company or the ship, personnel conducting internal audits of the security measures specified in the SSP or evaluating its implementation:

   i. Have knowledge of methods of conducting audits and inspections, and control and monitoring techniques;

   ii. Do not have regularly assigned security duties; and

   iii. Are independent of any security measures being audited.

5. If the results of an audit require amendment of either the SSA or SSP, the CSO submits the amendments to the MSC for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended SSP meets the applicable requirements. The CSO then completes the table to assure proper record of the audit, its findings, and the response to the findings are kept up to date.

{Note: Example table used to keep records of audits and response to audits.}

Audit Date	Audit Description	Findings	Response	Resolution Date	CSO/ Signature

4.5 TERMINAL/PORT/SHIP(s) SECURITY ASSETS

a. The CSO shall maintain communications with all ports that company ship visits to ensure maximum benefit from security assets are available and that security procedures are in place and conducted in accordance with company/ship requirements and applicable Security Levels.

b. In addition to above, all ports where the ship conducts full cargo operations shall have coverage, as deemed appropriate by [COMPANY], of shore security personnel and equipment, for the protection of all concerned. All embarkation/disembarkation port shore security personnel are contracted by the company and follow procedures in accordance with company/government requirements.

c. In the event that such security precautions cannot be provided, the ship shall ensure that in accordance with Security Levels, appropriate security procedures/tasks are established onboard and ashore to protect all interests. The SSO is also responsible for establishing and maintaining a working relationship with all port security personnel/assets and providing information updates to the Master.

d. When requested by the port, the company, or when required by the Port State, a declaration of security, between the ship and the terminal/port/authority, will be completed prior to commencing any cargo operations or loading of stores.

e. ***{Note: The company should address any other procedures for interfacing with port facility activities.}***

4.6 SECURITY INFORMATION

{Note: The company shall address procedures and practices to protect security sensitive information held in paper or electronic format.}

4.7 LEVEL 3 INSTRUCTIONS FROM CONTRACTING GOVERNMENTS

The SSO will:

a. Acknowledge receipt of security level 3 instructions received from a Contracting Government or designated authority while in port or prior to entering port. The CSO is also to be informed of any such instructions.

b. Confirm initiation of the implementation of the appropriate measures and procedures as detailed in the SSP to the PFSO.

c. Report any difficulties in implementation of appropriate measures and procedures. The SSO will co-ordinate with the PFSO to determine appropriate actions.

d. Have information onboard, to be made available to Contracting Governments upon request, indicating who is responsible for deciding the employment of the ship's personnel and for deciding various aspects relating to the employment of the ship

e. Report any information that might affect maritime security in the area to the CSO, and appropriate authorities.

f. ***{Note: The company shall add addition procedures for responding to any security instructions the flag or port control state may give at security level 3.}***

4.8 DECK LIGHTING

While in port, at anchor, or underway, the ships deck and over-side will be appropriately illuminated during periods of darkness and restricted visibility in accordance with the Security Level and the judgment of the Master; but not so as to interfere with required navigation lights or safe navigation.

4.9 DANGEROUS GOODS AND HAZARDOUS SUBSTANCES

{Note: The company should address procedures to establish, maintain, and update an inventory of any dangerous goods and hazardous substances carried on board, including their location.}

SECTION 5

DECLARATION OF SECURITY

a. ***{Note: The company should address procedures for requesting a Declaration of Security (DoS) and handling DoS requests from a facility or other ship.}***

b. At Security Level 1, a DoS is completed and signed by the Master, SSO, or their designated representative, with the SSO or PFSO, or their designated representative, of any ship or port facility with which it interfaces.

1. For a ship-to-facility interface, prior to arrival to a facility, the PFSO of the port facility and the Master, SSO, or their designated representatives coordinates security needs and procedures, and agree upon the contents of the DoS for the period of time the ship is at the port facility. Upon arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the PFSO of the facility or the Master, SSO, or designated representatives sign the written DoS.

2. For a ship-to-ship interface, prior to the interface, the respective Masters, SSOs, or their designated representatives coordinates security needs and procedures, and agree upon the contents of the DoS for the period of time the ships are interfaced. Upon the ship-to-ship interface and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, SSOs, or designated representatives sign the written DoS.

c. At Security Levels 2 and 3, the Master, SSO, or designated representative sign and implement a DoS prior to any ship-to-ship interface.

d. At Security Levels 2 and 3, the Master, SSO, or designated representative of any ship sign and implement a DoS with the PFSO of any port facility on which it calls prior to any cargo transfer operation or passenger embarkation or disembarkation.

e. At Security Levels 1 and 2, the SSO implements a continuing DoS for multiple visits with port facilities that are frequently interfaced provided that:

1. The DoS is valid for the specific Security Level;

2. The effective period at Security Level 1 does not exceed 90 days; and

3. The effective period at Security Level 2 does not exceed 30 days.

f. When the Security Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS is signed and implemented in accordance with this section.

g. The port authorities may require at any time, at any Security Level, to implement a DoS with the SSO or PFSO prior to any ship-to-ship or ship-to-facility interface when he or she deems it necessary.

SECTION 6

ACCESS TO THE SHIP

6.1 PHYSICAL ACCESS TO THE SHIP

a. COMPANY POLICY

It is [**COMPANY**] policy that all means of access to the ship are closed unless the Master decides there are operational reasons to have these open. All open access must be protected to the same standard.

Means of access include, but are not limited, to all

1. Access ladders
2. Access gangways
3. Access ramps
4. Access doors, side scuttles, windows, and ports
5. Mooring lines and anchor chains
6. Cranes and hoisting gear

b. OPERATIONAL DECISIONS AND SECURITY

The Master will 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 manpower allocation of security staff to ensure smooth operations and safe, secure movement of the ship's cargo.

c. RESPONSIBILITY FOR ACCESS/DOOR CONTROLS

The SSO reports to the Master for the overall security of the ship. The SSO will ensure the following is carried out:

- Patrols of the ship's decks observing any movements around the ship - both outboard and quayside.
- The regular checking, whether the doors be open or closed, of all ship side openings and its concomitant security implications.
- Inspection of focsle, mooring deck and other deck areas for any evidence of attempted unauthorized access.
- A thorough check to ensure that those doors that are open are manned by responsible personnel of the department conducting operations. (Unmanned open side port doors may be accepted if the side port opening is otherwise protected with a barrier that will prevent personnel from entering the ship.)

d. APPROVAL OF ACCESS/DOOR OPENING

While in port, no shell door will be opened under any circumstances without the express permission of the Officer of the Watch (OOW). At sea, no shell door will be opened without permission of the Master. Any shell door opened for any reason other than crew access will be manned by a responsible officer/person conducting the operation and who will be clearly visible at that location by means of wearing a High Visibility Vest. The only exception to this is where an approved barrier protects the opening.

The department head conducting operations shall ensure adequate relief of all watches. Under no circumstances are positions to be left unattended at any time for whatever reason until a relief has been briefed and taken over responsibility.

Security of the gangways is the primary responsibility of the SSO and the assigned security staff.

The Deck Department will man all access doors as required to support the SSO and the assigned security staff. The OOW will assist the SSO in ensuring that adequate manpower is provided to secure all access points.

The SSO shall coordinate security measures with each terminal operator, including security guards and barrier arrangements.

e. ROVING SECURITY PATROLS

While in port and at sea the SSO, in consultation with the Master, shall ensure that there are security patrols of all decks, commensurate with operational requirements.

f. BRIEFINGS

Security briefings are provided to all ship personnel on possible threats, the procedures for reporting suspicious persons/objects/activities, and the need for vigilance, in accordance with the applicable security level.

6.2 SEARCH PROCEDURES AND POLICIES

a. Searches of personnel seeking to board ship are conducted at the discretion of the SSO, in accordance with the applicable Security level. Persons refusing to comply with this policy will be denied access to the ship. Searches can be random and shall be undertaken by the port facility in close cooperation with the ship and in close proximity to it.

{Note: The company should set a frequency for these searches at each Security level.}

b. All items brought on board the ship are subject to control, monitoring, inspection and search. Persons refusing to comply with this policy will be denied access to the ship.

c. Everyone boarding the ship, including visitors, contractors, and crew are subject to be checked for the carriage of weapons, ammunition, incendiaries and explosives, narcotics and paraphernalia.

d. Carry-on articles will be inspected in accordance with the applicable Security Level.

e. A designated secure area on board or in liaison with a port facility is established to conduct inspections and screening of people, baggage (including carry-on items), personal effects, vehicles and the vehicles contents.

f. Ship personnel are not required to engage or be subjected to screening, or the person or of personal effects, by other ship personnel, unless security clearly requires it. Any such screening must be conducted in a way that takes into full account individual human rights and preserves the individual's basic human dignity.

g. In liaison with the port facility, ensure a defined percentage of vehicles to be loaded aboard car carriers, RO-RO and passenger ships are screened prior to loading

{The company should assign what percentage is appropriate}

h. Checked persons and personal effects are segregated from unchecked persons and personal effects.

i. In liaison with the port facility, ensure that all unaccompanied vehicles to be loaded on passenger ships are screened prior to loading.

6.3 PERSONNEL ACCESS TO THE SHIP

a. COMPANY POLICY

It is [COMPANY] policy that everyone will be required to have valid picture identification and be authorized ship access by authorized personnel, if deemed to have valid reason, in order to conduct their business.

Persons refusing to comply with company policy will be denied access to the ship and appropriate authorities will be informed for any further action deemed necessary. Appropriate authorities include the SSOs, the CSOs, the port authorities, and to the national or local authorities with security responsibility.

{This section should contain the company's procedures for reporting to the appropriate authorities. This should also include how to respond to the presence of unauthorized persons on board, including repelling unauthorized boarders.}

b. IDENTIFICATION SYSTEM

It is [**COMPANY**] policy to establish an identification system that, when practicable, is coordinated with the port facility. The identification system will be regularly updated, and abuse of procedures are subject to disciplinary action.

c. CREW IDENTIFICATION(s)

All crew will be in possession of a company identification pass, which is a tamper resistant pass made of a durable material and contains the information detailed below. The SSO is responsible for the issuance of all passes. The pass is required to be entered into the ship's security computerized system, which registers personnel onboard and provides picture identification on the computerized display screen.

Pass Information	**Crewman Permit Information**	
Name	Family Name	Weight
Photograph	Given Name & Initials	Sex
Home Address		
Nationality	**Passport Number**	
Company Name		
Expiration Date	Date & Place of Birth	
Rank/Rate		
Hair Color	Eye Color	
Height	Weight	
Bar Code		

CREW RECRUITMENT

The recruitment of all crewmembers shall be conducted by appropriate manning agencies approved by [**COMPANY**]. Background checks of all future employees shall be conducted and documentary evidence submitted before new hires are accepted for employment. The method of said background checks are as indicted below.

{Note: This section should document the sources (e.g., agencies, bureaus, and direct hiring processes) the company uses to recruit new crewmembers. For each of the sources, the information provided here should define the level of background checks (e.g., criminal record or police checks) that are required for a person to qualify for employment.}

d. COMPANY IDENTIFICATION PASSES/CONTROL AND BOARDING PROCEDURES

1. The SSO is responsible for issuing permanent company identification cards.
2. Company identification cards made on board will be permanent for one year from date of issue. They will be issued to the ship's crew, certain approved shore staff, agents, members of their staff and selected contractors, all to be approved by CSO. The issue of permanent company identification to family members is strictly forbidden.
3. Any member of the ship's company whose contract expires, or is terminated will have their pass withdrawn before issue of their passport upon leaving the ship, or when the expiration date on the pass comes into effect.
4. Replacement for a lost company identification card will be issued by the SSO after the appropriate investigation and action has been carried out by the head of the responsible department. A copy of the formal warning (if issued), or letter of explanation by the head of department is to be presented to the SSO before issue of pass.

   A subsequent loss of Company identification card will result in the issue of a formal (written) personnel warning under the company's procedures.

e. VISITOR PASSES/CONTROL AND BOARDING PROCEDURES

There is a visitor's policy for all crewmembers per company procedures based on the Security levels.

1. Crewmembers are only permitted to have visitors at turnaround ports in which case a visitor's pass will be issued by the SSO after approval by the Master.
2. Visitor passes will be issued for contractors and Port Agents not entitled to a permanent pass. Visitor passes will be issued by the SSO upon notification by the requesting Security Manager.
3. These passes will be handed to the visitor when they arrive at the gangway on production of valid photographic identification. This identification will be returned to the owner upon surrender of the visitors pass when leaving the ship.
4. The issuing authority may authorize a visitor to have frequent access to the ship. It is the SSO's responsibility to operate this system and the Master will ensure that all departments cooperate fully with management's instructions.
5. The Master always has discretion to approve passes to meet any special circumstances.

f. VISITOR PASS IMPLEMENTATION GUIDELINES

1. Visitor's passes must be issued in accordance with a ship procedure that meets the company security requirement.
2. Notification of all visitors is to be submitted to the SSO at the earliest opportunity and prior to the ship's arrival at visitation port. Valid government photographic identification must be surrendered at the gangway in exchange for a visitors pass. All official(s), not previously issued permanent Company identification card identification must be met at the gangway by a representative of the department with whom they have business, and be escorted at all times while onboard. All visitors are to note the terms and conditions for issuance of the visitors pass, and are required to sign prior to receipt of the pass.

3. Visitor passes are to be kept inside the gangway security storage, except when issued, and the locker is to be kept secure at all times. The security staff member is to identify every pass not handed in at appropriate time and make a report to the SSO before ship's departure. The SSO is to ensure all officials and other visitors are ashore prior to ship's departure. Any missing/lost passes are to be recorded and appropriate action taken.

4. Visitors arriving at the gangway on business and who are not expected are to be requested to wait, as the security staff member checks with the appropriate Head of Department. Upon receipt of the officers clearance he may issue a visitor passes in exchange for valid photographic identification. A member of the appropriate department must attend at the gangway in order to escort the visitor. In the event the security staff member is unable to contact the required Head of Department/Deputy, they may gain approval from the SSO or OOW. All visitors are to note the terms and conditions for issuance of the visitors pass, and are required to sign prior to receipt of the pass.

5. The only exceptions to the rule are as follows:

   Officials in uniform/plain clothes with positive photographic identification of their position, e.g., Customs, Immigration, Health, Agriculture, do not require visitor passes. An Officer of the appropriate department must meet and escort these officials.

6. The SSO or OOW is to be called if a security staff member is in doubt about the issuing of visitor passes for any individual.

7. Visitors are not permitted while conducting tender service, unless specifically authorized for organized functions by the company.

8. At ports that the ship visits regularly, temporary company identification cards (good for one year) may be issued as before to agents/tour operators/contractors etc., upon authorization from the CSO.

g. STEVEDORE IDENTIFICATION AND CONTROL

1. The control and identification of all stevedores is the responsibility of the terminal operator. This does not exclude identification check by security staff for stevedores boarding the ship.

2. Maximum efforts are made by the CSO and the SSO to ensure all ports maintaining adequate controls on employee identification, and control access to port restricted areas.

3. When on board, stevedores will remain in their designated work areas and are not allowed unescorted/unrestricted movement around the ship. If found unescorted in unauthorized areas they are to be challenged and escorted back to their designated work area. Stevedores are not permitted to use onboard crew dining facilities.

SECTION 7

RESTRICTED AREAS

7.1 RESTRICTED AREA POLICY

It is [**COMPANY**] policy that all designated restricted areas are locked, unless the Master, or in the case of the engine control room and engine room the Chief Technical Officer, decides that for operational reasons it is necessary to have them unlocked. Restricted areas will be inspected during each security patrol.

The following have been designated as Restricted Areas:

a. The Bridge

b. The Communications Center.

c. Engine Room/Engine Control Room.

d. Rear Steering Flat

e. Bow Thruster Room.

f. Control Rooms for Fire Fighting Equipment.

g. Emergency Generator Room.

h. Computer Rooms

i. Security Office & Central Surveillance Monitoring Station.

7.2 DESIGNATED RESTRICTED AREA SIGNS

Each Designated Restricted Area is distinctly marked with a placard mounted at eye level at least 20-cm high by 30-cm wide with the words "RESTRICTED AREA AUTHORIZED PERSONNEL ONLY" in red letters at least 5-cm high on a white background. The sign should also indicate that unauthorized presence within this area constitutes a breach of security.

7.3 COMPANY POLICY REGARDING ACCESS TO RESTRICTED SPACES

Restricted areas shall only be accessed by ship's company; company shore staff, contractors, vendors, and other visitors as authorized by the Master. All restricted areas are secured by means of door lock keypad, the combination of which is changed quarterly and after every dry and wet dock availability period. Combinations are only issued to personnel authorized access to these restricted spaces. All other areas without such locks are to be secured by means of key lock. Access to keys is permitted to only authorized personnel.

7.4 VULNERABLE POINTS

In addition to the areas designated as Restricted Areas, there are a number of additional areas that have been classified as vulnerable points. All these areas are kept locked.

a. Air Conditioning Plant and Fan Room

b. Battery and Accumulator Room

c. Electrical Stations

d. Hydraulic Room, including hydraulic controls for shell gates

e. Lift Machinery Spaces

f. Bottled Gas Stores

g. Paint Shop

7.5 SMALL TECHNICAL LOCKERS

The many small technical lockers situated throughout the ship are protected by a number of measures to be used at the discretion of the Master particularly when there is a change in the Security Level.

7.6 MASTER KEYS AND KEY CARDS

{Note: This section should indicate all of the locations for and responsibilities for control of sets of keys, master keys, and other access control systems (e.g., key cards).}

7.7 LOST/STOLEN KEYS TO RESTRICTED AREAS

a. The loss or theft of keys to any restricted area is to be immediately reported to the Master and OOW who shall take appropriate action to ensure said area is secured and prevent unauthorized access. An immediate investigation into the loss or theft of key(s) shall be initiated.

b. In either of the cases above, a written report, stating the circumstances surrounding the loss or theft is to be submitted by the individual responsible for the key, to the Master within 24 hours.

c. Completion of investigation of the loss or theft of key(s) is established by presentation of the case to the Master with findings, conclusions and recommendations.

d. In the event that findings conclude that a theft occurred, the Master is to submit a report to the CSO at the first available opportunity.

SECTION 8

HANDLING OF CARGO

8.1 ACCESS TO CARGO AREAS

a. All cargo spaces are checked prior to cargo handling operations.

b. Access to cargo is restricted at sea.

c. Access to areas containing dangerous or hazardous cargo is strictly controlled.

d. Cargo handling equipment is secured when not in use.

8.2 CARGO IDENTIFICATION AND LABELING

a. All cargo is subjected to visual and physical examination, detection devices such as scanners, and canines to verify that the cargo being loaded matches the cargo documentation.

b. The container identification number of all loaded containers are verified against the manifest.

c. The container identification number of all empty containers are subjected to random verification against the manifest.

d. Non-containerized cargo is subjected to random verification against the manifest.

8.3 CARGO SEARCH PROCEDURES AND POLICIES

a. All cargo and cargo transport units are checked prior to and during cargo handling operations.

b. All cargo and cargo transport units are subject to be checked for the carriage of weapons, ammunition, incendiaries and explosives, narcotics and paraphernalia.

c. Random inspections are conducted on at least 25% of the cargo being loaded using scanning/detection equipment, mechanical devices, or canines.

d. If an agreement has been established with the shipper or other responsible party covering off-site checking, sealing, scheduling, supporting documentation, etc., such arrangements will be communicated to and agreed with the PFSO concerned.

e. In liaison with the facility, ensure percentage of vehicles loaded aboard car carriers; RO-RO and passenger ships are screened prior to loading

{The company should assign what percentage is appropriate}

8.4 CARGO TAMPER PREVENTION

a. Seals on containers and other cargo lockers are checked, in liaison with the port facility, to prevent tampering, in accordance with the applicable security level.

SECTION 9

DELIVERY OF SHIP'S STORES

9.1 STORES LOADING

a. Stores deliveries are checked to confirm that stores presented for delivery are accompanied by evidence that they have been ordered by the ship, to prevent ship's stores from being accepted unless ordered.

b. All stores are checked to verify that stores match the order prior to being loaded on board.

c. All stores are inspected for package integrity prior to being loaded on board, in accordance with the applicable Security level.

d. All stores are controlled or immediately stowed in secure areas following delivery.

9.2 STORES INSPECTION

a. All stores and provisions are subjected to visual and physical examination, in accordance with the applicable Security level.

9.3 STORES SEARCH PROCEDURES AND POLICIES

a. All stores are subject to checks for the presence of weapons, ammunition, incendiaries and explosives, narcotics and paraphernalia.

b. Random screenings may be conducted on the stores being loaded using scanning/detection equipment, mechanical devices, or canines.

9.4 TAMPER PREVENTION

a. Stores are stowed in restricted areas.

b. A watch is maintained for unauthorized removal of ship's stores.

SECTION 10

HANDLING UNACCOMPANIED BAGGAGE

10.1 UNACCOMPANIED BAGGAGE POLICY

It is [COMPANY] policy that all unaccompanied baggage, including personal effects, which is not with a member of the ship's personnel is identified and subjected to appropriate screening, including searching, before it is accepted on board the ship.

10.2 INSPECTING UNACCOMPANIED BAGGAGE

a. All items brought on board the ship are subject to control, monitoring, inspection and search, in accordance with the applicable Security level.

b. All unaccompanied baggage is checked for the presence of weapons, ammunition, incendiaries and explosives, narcotics and paraphernalia, in accordance with the applicable security level.

c. All unaccompanied baggage is handled securely after screening.

SECTION 11

MONITORING THE SECURITY OF THE SHIP

11.1 SECURITY EQUIPMENT

a. The SSO is responsible for the storage and control of all shipboard security equipment, including the identification card system.

b. All security equipment is serviced, maintained, and repaired in accordance with manufacturers' recommendations. This ensures the equipment will perform continually (including consideration of the effects of inclement weather conditions and power disruptions).

{Note: The company should add the specific maintenance requirements.}

c. All security equipment is inspected, tested, and calibrated in accordance with manufacturers' recommendations.

{The company should address the procedures and frequency for inspection, testing, calibration, and maintenance of any security equipment provided on board.}

d. Maintenance, repair, and inspection/testing records for security equipment are maintained by the SSO.

e. Any equipment or system failure or malfunction shall be reported immediately.

Device	Location

{Note: All security devices and their locations are to be listed in the table.}

11.2 CLOSED CIRCUIT TELEVISION CAMERAS

One closed circuit TV camera is mounted on each bridge wing, and the monitor with remote control for the cameras is located in the Security Center on the bridge. Additional cameras are also fitted at all shell doors with a central monitoring station provided for surveillance during periods determined by the Master, in accordance with the applicable Security level. Recordings shall be maintained for a period of seven (7) days.

11.3 ALARM SYSTEMS

a. All critical shipboard areas are alarmed as appropriate and monitored by relevant departments.

b. Alarms activate an audible or visual alarm when an intrusion is detected and sound in a location that is continuously staffed by personnel with security responsibilities.

c. All security alarm systems are subject to periodic testing. Such testing is documented and reflects consideration of manufacturer's recommendations and the specific installation/application on the ship.

d. Information regarding all actuations of security alarms and inoperative security alarms are submitted to the SSO.

e.

Alarm System	Activation Point Location

{Note: This table should address each alarm system provided on board and the location of its activation point. This table may be kept elsewhere on board in a document known to the master, SSO, and other senior shipboard personnel, as decided by the Company.}

f. ***{Note: The company should include specific procedures, instructions, and guidance on the use of the ship security alarm systems, including its testing, activation, deactivation, and resetting, as well as limiting false alerts.}***

11.4 ELECTRONIC DEVICES AT MAIN EMBARKATION PORTS

Device	Number Held On Board	Usage	Operator

{Note: This type of table should be provided to indicate what types and amount of security equipment (if any) are available and what functions they provide. }

11.5 PROCEDURES FOR USE OF SECURITY EQUIPMENT

{Note: This section should provide specific procedures for how to use any of the type of security equipment that is employed on board the ship. Much of this type of information can be drawn from manufacturer's instructions provided with the equipmentIf this information is included in a security training manual rather than being in the (ssp), then that document can be referenced for such detailed instructions.}.

{Note: The Ship Security Alert System is a specific item of equipment that this section should address. The information provided should:

- ***identify where the ship security alert system activation points are***
- ***provide procedures for the use of the ship security alert system, including the activation, deactivation and resetting of the alarm***
- ***provide a procedure to allow testing of the alarm without creating a spurious security alarm}***

11.6 SEARCHES

At all times ship personnel, which may be in coordination with a facility, are prepared to conduct emergency searches of the ship.

SECTION 12

COMMUNICATIONS

12.1 An effective two-way communication system with the CSO is provided so that any unlawful act against the ship or person can be reported immediately using the appropriate format. This report is required both in places subject to the jurisdiction of the United States and places outside the jurisdiction of the United States and must provide the following information:

a. Location of ship (Lat/Long/Time)

b. Name/Nationality/Dates and Place of Birth of Victim

c. Name/Nationality/Dates and Place of Birth of Person(s) committing unlawful act.

d. Nature and extent of severity of injuries sustained, if any.

12.2 VHF radios are employed as the primary means of communication, with ship intercom/phone used as a backup. Maintain radio contact during operations:

a. Within the ship – radio contact will be maintained between bridge or control room for all ingress and egress points.

b. Between ships – radio contact will be maintained between ships in port at all times to relay security concerns.

c. Between ship and port – radio contact will be maintained between Port Personnel and Company Representatives at all times to relay security concerns.

12.3 Privately owned, hand held radio communication devices are not authorized for use on board this ship. Failure to comply will result in confiscation and retention of radio.

12.4 Distress and Duress: Procedures for indicating that the SSO or Security Officer is in distress, or is communicating under duress are the responsibility of the SSO. Appropriate ship's personnel are trained in these procedures.

12.5 Communications with terminal operator's personnel will be coordinated through the ship's agent with preference given to VHF radio and/or telephone. For security purposes, direct communications links are established between ship security personnel and the security personnel in the port facility. Those links are subject to periodic testing and failure to maintain communication are to be reported immediately to the SSO.

12.6 SSOs communicate directly with the CSO, via telephone or e-mail as necessary to co-ordinate shipboard security operations and support requirements, and provide updated port contact information.

12.7 EXTERNAL COMMUNICATION SYSTEMS

RADIO COMMUNICATION

a. Ship's Call Sign

Satcom Numbers: Telephone:

Fax:

Telex:

IMO No:

b. Equipment On Board:

{Note: This section should list the specific types of communication equipment onboard, including equipment used for communication with port/coastal authorities, the flag administration, and company organizationsThis may include satellite and other communications systems. Communications equipment for lifeboats and for coordination with helicopters (if appropriate) should also be addressed.}.

12.8 INTERNAL COMMUNICATION SYSTEMS

[Note: This section should describe each of the forms of internal communications systems (e.g., telephones, public address systems) the ship has.]

12.9 SHIPBOARD/INTERNAL RADIO COMMUNICATION

[Note: This section should describe each of the forms of internal radio communications systems the ship has and how those resources are distributed.]

SECTION 13

SECURITY INCIDENT PROCEDURES

13.1 For each Security Level, the ship owner or operator will ensure the SSO and ship security personnel are able to:

a. Respond to security threats or breaches of security and maintain critical ship and ship-to-facility interface operations, including:

1. Prohibiting entry into affected area;
2. Denying access to the ship, except to those responding to the emergency;
3. Implementing Security Level 3 security measures throughout the ship;
4. Stopping cargo-handling operations; and
5. Notifying shoreside authorities or other ships of the emergency;

b. Evacuating the ship in case of security threats or breaches of security;

c. Reporting security incidents including:

i. Notification of suspicious activities

ii. Notification of breaches of security

iii. Notification of transportation security incident (TSI)

d. Briefing all ship personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

e. Securing non-critical operations in order to focus response on critical operations.

13.2 The Master or SSO are responsible for filling out and submitting security incident reports to the CSO within 24 hours of the discovery of any unlawful act. The following Report Format is to be used:

a. SHIP OR PORT AREA DESCRIPTION

Name of Ship:

Flag:

Master:

Port Facility Security Officer:

Ship Security Officer:

b. BRIEF DESCRIPTION OF INCIDENT OR THREAT

c. DATE, TIME, AND PLACE (Lat/Long) OF INCIDENT OR THREAT:

d. NUMBER OF ALLEGED OFFENDER(S)

Crew: Other:

e. DETAILS OF OFFENDER(S)

Name: Nationality: DOB/POB

Name: Nationality: DOB/POB

Name:	Nationality:	DOB/POB
Name:	Nationality:	DOB/POB

f. NUMBER OF ALLEGED VICTIM(S)

Crew: Other:

g. DETAILS OF VICTIM(S)

Name:	Nationality:	DOB/POB
Name:	Nationality:	DOB/POB
Name:	Nationality:	DOB/POB
Name:	Nationality:	DOB/POB

h. NATURES AND SEVERITY OF INJURY SUSTAINED

Name:	Injury:
Name:	Injury:
Name:	Injury:
Name:	Injury:

i. TYPE OF DANGEROUS SUBSTANCES OR DEVICES USED (FULL DESCRIPTION)

Weapon:

Explosives:

Other:

j. METHOD USED TO INTRODUCE DANGEROUS SUBSTANCES OR DEVICES INTO THE PORT FACILITY OR SHIP

Persons:

Baggage:

Cargo:

Ship Stores:

Other:

a) Where were the devices/items described concealed?

b) How were the items described in Section 5 used and where?

c) How was the security measures circumvented?

k. WHAT MEASURES AND PROCEDURES ARE RECOMMENDED TO PREVENT A RECURRENCE OF A SIMILAR EVENT?

l. OTHER PERTINENT DETAILS (Use additional sheets if required)

m. Upon receipt of a security incident report, the CSO files a written report of said incident, to the appropriate authorities.

{Note: In a specific security plan, the organizations should be identified and how the report is to be delivered should be specified.}

.SECTION 14

SPECIFIC SECURITY ACTIONS TO BE IMPLEMENTED BASED ON THE SECURITY LEVEL

This section defines the specific security measures the ship will implement at each security level. It represents the results of the ship-specific security assessment, taking into account international requirements and applicable regulatory guidance. When this information indicates that a specific measure is implemented at more than one security level, it is likely that the degree of detail or frequency of the measure is increased at the higher security levels.

Table 1 General Requirements for Security

	Security Level		
Protective Measure	**1**	**2**	**3**
All ship crewmembers will review and exercise their security duties and responsibilities through drills and training.	YES*	YES*	YES*
Provide security information to all crewmembers and any security personnel that includes the security level and any specific threat information.	YES	YES	YES
SSO will communicate with the port and specific waterfront facility to coordinate protective measures.	YES	YES#	YES#
* Drills and exercises are conducted quarterly.			
# Coordinate additional protective measures.			

Table 2 Measures for Ensuring Port-Specific Security Communication

	Security Level		
Protective Measure	**1**	**2**	**3**
Perform regular communications checks	YES	YES	YES
Provide a backup means of communication	YES	YES	YES#
# Provide a redundant and multiple means of communication			

Table 3 Security Requirements for Monitoring Restricted Areas to Ensure That Only Authorized Personnel Have Access

	Security Level		
Protective Measure	**1**	**2**	**3**
Locking or securing access to *restricted areas*[@]	YES	YES‘	YES‘
Monitoring and using surveillance equipment	YES	YES**	YES[1]
Using personnel as security guards or patrols	YES	YES*	YES[#]
Using automatic intrusion detection devices, which if used must activate and audible and/or visual alarm at a location that is continuously attended or monitored, to alert personnel to unauthorized access.	YES	YES	YES
Restricting access to areas adjacent to access points	NO	YES	YES***

‘Increasing the frequency and intensity of monitoring and access controls on existing restricted areas

* Dedicating additional personnel to guarding or patrolling restricted areas;

** Providing continuous monitoring of each area, using surveillance equipment

Posting personnel to continuously guard restricted areas and/or assigning personnel to continuously patrol restricted areas and areas adjacent to restricted areas.

@ Doors in escape routes must be capable of being opened without keys from the direction for which escape is required.

*** Restricting access to additional areas

[1] Switching on all surveillance equipment capable of recording activities on, or in the vicinity of, the ship and maximizing the length of time such surveillance equipment can continue to record

Table 4 Measures for Controlling Access to the Ship

{The following protective measures should be applied at the appropriate access locations at each security level, the types of restrictions to be applied, the means of enforcing them, and the frequency (random or occasional basis) of the application of these measures; all to be set by the company}

	Security Level		
Protective Measure	**1**	**2**	**3**
Access points are secured[@] or continuously attended to prevent unauthorized access.	YES	YES[#]	YES[#]
Lock or otherwise prevent access to unattended spaces that adjoin areas to which passengers and visitors have access[1]	YES	YES	YES
Weather-deck access vents, storage lockers, and doors to normally unmanned spaces (such as storerooms, auxiliary machinery rooms, etc.) are locked[@] or precautions taken to prevent unauthorized access.	YES	YES	YES
Limit entry to the ship to a minimum number of access points.[+]	NO	YES	YES*
Establishing a restricted area on the shoreside of the ship, in close cooperation with the port facility.	NO	YES	YES
Carrying our a full or partial search of the ship	NO	YES	YES**
Moving the ship	NO	NO	YES
Evacuating the ship	NO	NO	YES
Initiating measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.	NO	NO	YES

* Limit entry to a single access point when possible.

@ Doors in escape routes must be capable of being opened without keys from the direction for which escape is required.

\+ While not restricting egress from the ship in the event of an emergency.

\# Assign additional personnel at appropriate access points as designated in the security plan.

** Preparing for a full or partial search of the ship and searching restricted areas as part of the search

Table 5 Measures for Monitoring Deck and Areas Surrounding the Ship

	Security Level		
Protective Measure	**1**	**2**	**3**
Use security lookouts and/or security patrols	NO	YES*	YES*
Light deck and ship access points during the period between sunset and sunrise and periods of limited visibility sufficiently to allow visual identification of persons seeking access to the ship@	YES	YES**	YES***
In port – Light is provided to allow crewmembers to see beyond the ship, both pier side and waterside; including areas on and around the ship	YES	YES**	YES***
Underway - maximum lighting available consistent with safe navigation and international regulation	YES	YES**	YES***
In liaison with the port facility, perform waterside boat patrols to deter waterside access to ship and foot patrols or vehicle patrols on the shore side	NO	YES	YES#
Use divers to inspect the underwater pier structures prior to the ship's arrival, upon the ship's arrival, and in other cases deemed necessary and prepare for underwater inspection of the hull	NO	NO	YES#

@ Coverage may be provided in coordination with a facility

* Increase the number and frequency of:

- security patrols during periods of reduced ship operations to ensure continuous monitoring; and
- waterside boat patrols to ensure continuous monitoring.

** At these higher security levels, additional lighting will be coordinated with the waterfront facility to provide additional shore side lighting. Additional lighting may include:

- using spotlights and floodlights to enhance visibility of the deck and areas surrounding the ship; and
- using lighting to enhance visibility of the surrounding water and waterline.

If required by port facility or if in response to specific threat information.

*** Switching on all lights, illuminating the vicinity of the ship

Table 6 Measures For Controlling The Embarkation Of Persons And Their Effects

	Security Level		
Protective Measure	**1**	**2**	**3**
Verify reason personnel are embarking the ship by using joining instructions, tickets, boarding passes, work orders, pilot orders, surveyors orders, visitor badges, government identification, or other means.	YES	YES	YES
Segregate embarking passengers from disembarking passengers	YES	YES	YES
Suspending embarkation and disembarkation	NO	NO	YES
Positively identify crewmembers, vendors, visitors, and other personnel prior to each embarkation.	YES	YES	YES
Denying access to visitors who do not have a verified destination	NO	YES	YES
Verify arriving crew as authorized to serve aboard the ship.	YES	YES	YES
Inspect persons, baggage, carry-on items, and personal gear for *prohibited weapons*, incendiaries, and explosives.	YES#	YES@	ALL
Security briefings provided to all persons on board, prior to departing, on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities.	NO	YES	YES*
Assign personnel to guard designated *inspection* areas.	NO	YES	YES
Limit entry to only crewmembers and other authorized personnel.	NO	YES	YES***
Escort all service providers or other personnel needed aboard to provide essential services to the ship.	NO**	YES**	YES**

* Security briefings are generally provided to all crew members, prior to each embarkation and disembarking.

This may be accomplished by random *inspection*s, such as 5-20% or some other method addressed in the ship security plan.

@ Increase the frequency and detail of screening people, personal effects, and vehicles being embarked or loaded onto the ship *{The company should note what increase is appropriate for Security Level 2}*

** All personnel allowed onboard are identified and approved at all security levels.

***Access is granted only to those responding to the security incident or threat there of and being prepared to cooperate with the responders and facilities.

Table 7 Measures for Supervising the Handling of Cargo and Ship's Stores

	Security Level		
Protective Measure	**1**	**2**	**3**
Routinely check cargo, ship stores, and cargo spaces prior to and during cargo handling	YES	YES*	YES*
Use of scanning/detection equipment, mechanical devices, or canines to check cargo.	YES	YES#	YES
Coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures	YES	YES#	YES
Verify non-containerized cargo against the manifest	YES	ALL	ALL
Verify the container identification numbers of loaded containers against the manifest	ALL	ALL	ALL
Verify the container identification numbers of empty containers against the manifest	YES	ALL	ALL
Inspect ship's stores and provisions	YES#	YES+	ALL
In liaison with the facility, ensure a defined percentage of vehicles to be loaded aboard car carriers, RO-RO and passenger ships are screened prior to loading ***{The company should assign what percentage is appropriate}***	YES	YES#	YES
In liaison with the facility, check seals or other methods used to prevent tampering	YES	YES#	YES
Restricting or suspending cargo and ship store operations	NO	NO	YES
Refusing to accept ship stores on board	NO	NO	YES
Being prepared to cooperate with responders and facilities	NO	NO	YES
Verify the inventory and location of any hazardous materials carried on board	NO	NO	YES
* Increasing the frequency and detail of checking cargo, ship stores, and cargo spaces. This will ensure that only the intended cargo, container, or other cargo transport units are loaded			
# Increase the frequency ,detail, and/or enhance			

Table 8 Measures for Handling Unaccompanied Baggage

	Security Level		
Protective Measure	**1**	**2**	**3**
Ensure the checking of all unaccompanied baggage	YES	YES	YES
X-ray screening of all unaccompanied baggage	YES	YES	YES#
Preparing to restrict or suspend handling of unaccompanied baggage	NO	NO	YES
Refuse to accept unaccompanied baggage on board	NO	NO	YES
# More extensive screening, x raying from two or more angles for example			

SECTION 15

SCREENING FOR WEAPONS, INCENDIARIES, AND EXPLOSIVES

15.1 Screening procedures are conducted in accordance with Security Levels; all screening areas are designated restricted in order to minimize tampering with items during and after screening. Although landside screening is generally preferred, the screening of smaller items (i.e. personal effects, baggage, individually packaged stores) need not take place outside the boundaries of the ship provided that the screening area onboard the ship is adequately restricted and suspicious items can be removed prior to stowage. Screening may be conducted by manual, canine, electronic, or other equivalent means.

15.2 Screening systems should be capable of detecting prohibited weapons, incendiaries and explosives. The routine use of a combination of screening systems, or the use of one system that is effective at detecting the full range of prohibited items, is preferred at all Security Levels.

15.3 In accordance with certain international requirements, a female security staff member will be trained and certified to conduct screening of female crew (if any), commensurate with applicable Security Levels.

15.4 Anyone refusing to submit to security screening at a point of access shall not be allowed to board the ship and will be reported to the appropriate authorities.

15.5 FIREARMS

UNLESS APPROVAL IS GRANTED BY THE COMPANY SECURITY MANAGER, WEAPONS ARE STRICTLY FORBIDDEN ONBOARD ANY SHIP, OR ONTO THE DOCK AREA.

AN EXCEPTION TO THIS POLICY ARE LAW ENFORCEMENT AGENCY PERSONNEL ACTING IN OFFICIAL CAPACITY AND WITH FULL PERMISSION OF THE SHIP MASTER

15.6 LIAISON WITH LAW ENFORCEMENT AGENCIES

The SSO will establish and maintain liaison with local law enforcement agencies to ensure that their full protective capabilities are deployed in the protection of the ship when operating under heightened Security Levels.

SECTION 16

GANGWAY AND GANGWAY CONTROL

16.1 The gangways are manned by a Security Officer who is responsible to the SSO or OOW. Their primary responsibility is to control access to the ship, and ensure the safety and security of the gangway area. Nothing is to hinder the Security Officer in the performance of these duties and, if necessary, they are to call the SSO or OOW for assistance.

16.2 When appropriate, additional staff may be required to ensure disruption or delay of embarkation/disembarkation at the gangway. Whenever possible the need for those extra personnel will be arranged in advance by the Master in consultation with the SSO.

16.3 Personnel detailed for gangway duty are given Standing Orders for their instruction and guidance. The following is an outline of what should be included in these Standing Orders:

a. All gangway personnel are responsible to the SSO or OOW and must notify them if in doubt on any matter by telephoning appropriate number or by hand radio.

b. Those on gangway duty must not leave the station until properly relieved.

c. No one is to be permitted to board without one of the valid company passes, as identified in the company procedure on passes.

d. All persons boarding and leaving the ship must be asked to produce appropriate identification.

e. The gangway must be checked to see that it is properly lashed and secured, well lit and at all times safe for use.

f. An alert watch is to be kept at all times at the head of each gangway. This watch must ensure that the gangway in use is operating within its permitted angles of elevation and that it can range freely with the tide or harbor swell

g. A watch shall be maintained for unauthorized removal of the ship's equipment and stores.

h. All communication devices are to be tested at least once per watch.

16.4 SECURITY OFFICER STANDING INSTRUCTIONS

a. Security Officers are responsible to the SSO or OOW for all matters regarding safety and security in the area of the gangway.

IN THE EVENT OF AN EMERGENCY SITUATION, SECURITY OFFICERS SHOULD, WITHOUT JEOPARDIZING THEIR OWN SAFETY, ALERT THE SSO OR OOW THEN THE MASTER DIRECT, AND OTHER RELEVANT OFFICERS AS APPROPRIATE.

b. An alert watch is kept at all times at the head of each gangway. This is to include careful scrutiny of the quayside area and, in particular, any movements of personnel in the areas of open shell doors and mooring lines fore and aft.

c. Company Procedure 4.6 refers to visitors to the ship and Standing Orders for gangway personnel. All Security Officers must be thoroughly familiar with these orders that are available from the Master. All persons boarding and leaving the ship are asked for their Cruise Card/Company identification card or Visitor's Pass or other forms of relevant identification.

d. Strict access control procedures are maintained on the gangway at all times, especially during embarkation/disembarkation. If, at any time, there is a hold up, either ashore, on board or on a pontoon, the crew is directed to wait in the foyer or on the launch and not on gangways/pontoons.

e. Gangways are not left unattended at any time for whatever reason until a relief has been briefed and taken over responsibility.

f. Crew members (Subject to Security Level) from another of the Company's ships may, be allowed on board upon presentation of a valid ID card and photographic identification. Crewmembers from any other shipping company ships are to be politely denied access; the need for security may be stressed to explain this refusal.

g. Gun port doors are closed or secured by approved methods at all times when not in use. The SSO or OOW is informed immediately if any are observed to have been left open and unattended/secured.

h. The SSO or OOW is informed immediately of any instance of persons boarding or leaving the ship other than by the gangway, i.e., leaping into storing doors/down conveyors etc.

i. Visitors passes are kept secure at all times. They are not left lying in the gangway area where they can be mislaid/stolen. On departure from every port all visitors' passes are taken from the gangway area and left in the Security Office for security. The gangway security stowage is kept locked at all times when not in use.

j. Deck Standing Orders in conjunction with these orders, deal with Visitors Passes and Routines and are strictly followed at all times.

16.5 OFFICERS IN CHARGE OF SHORE PARTY

a. **IN THE EVENT OF AN EMERGENCY SITUATION YOU SHOULD, WITHOUT JEOPARDIZING YOUR OWN SAFETY, ALERT THE SHIP'S BRIDGE BY RADIO IMMEDIATELY**, and any other relevant officer you can raise by any means at your disposal.

b. A security check is carried out **BY THE PERSON DELEGATED IN CHARGE OF THE SHORE PARTY.** This entails checking the Company identification card(s) of **ALL** crewmembers **PRIOR** to them boarding the launches to the ship. In the event of a crewmember failing to have his/her company identification card, their positive identification can be checked against the crew list provided in the Shore Party folder. Any crewmember without a company identification card should be (after I.D. Check) reported to the SSO or Security Officer conducting duties at the pontoon area, so that appropriate action may be taken prior to their arrival back on board.

c. Remember that security is an essential part of the smooth running of the shore party and depends on **YOUR** organization.

d. All persons embarking and disembarking from the tender **MUST** do so by the cab entrance. It is a disciplinary offence to board by any other means than the cab entrance and any offender is to be reported to the Bridge.

e. Your Hand Held Radio is your link with the ship. All messages on the radio are to be prefixed by **"BRIDGE - SHORE PARTY."**

f. Radio checks are conducted upon assuming duties and responsibilities of Officer in Charge of Shore Party. Checks are to include that batteries have sufficient power and radios are fully functional.

g. All reasonable measures are to be taken to ensure that the embarkation/ disembarkation area is kept clear of all obstacles (personnel/mechanical).

h. Adequate lighting is maintained quayside when conducting nighttime tender operations.

i. Crew visitors are not permitted onboard when operating tender service, unless specifically authorized for organized functions by the company.

SECTION 17

CONTINGENCY PROCEDURES

17.1 GENERAL REQUIREMENTS

The following procedures are followed in unusual circumstances that present a threat to the security of the ship:

17.2 Bomb Threats/Searches

17.3 Evacuation of the Ship

17.4 Response to Breach of Security or to Suspicious Activity on, or near, the Ship (including provisions for maintaining critical operations of the ship)

17.5 Security Procedures While in Dry-dock or Extended Maintenance

17.6 Procedures and Security Measures when Ship is at a Higher Security Level than the Facility

17.7 Procedures and Security Measures when Ship is at Port Which is not a Contracting Government

However, it is recognized that not all contingencies can be planned for in advance, so the Master, the SSO, and security staff members are authorized to take the actions they deem necessary for the safety of the ship and crew in situations where these procedures do not apply.

17.2 GENERAL BOMB SEARCH ROUTINE

Bomb searches are conducted by personnel familiar with the area(s) being searched. When conducting searches, personnel look for anything new or something unusual in their area. Trying to remember seeing anyone the previous day or anyone who does not normally appear in that area.

Any suspicions circumstances are immediately reported to the Bridge**,** the Secondary Command Center, or the Main Fire Station. The person involved should make all reports so that there is no miscommunication. Radio communications should not be used.

When the Bridge or Secondary Command Center receives a confirmed report of a suspicious item or package, the Master will decide on what action is to be taken with regard to evacuation from the area.

If a suspicious item/package is found:

a) Do not attempt to move or interfere with in any way

b) Do not put water over it

c) Use mattresses and/or sandbags to minimize blast effects, but do not cover it up.

d) Consider closing selected fire doors to minimize the effect of a blast.

e) Bear in mind that there may be more than one bomb.

f) Inform the company/authorities of the bomb’s description and location.

g) If at sea, head for a mutually agreeable port.

17.2.1 Bomb Search Routine in Port

{Note: This section should define the bomb search procedure for when the ship is in port. That procedure must reflect the specific staffing and arrangement of the ship, along with any security equipment (e.g., explosive vapor detectors) that the ship has. For in-port situations, the possibility of evacuation should be considered in the procedure.}

17.2.2 Bomb Search Routine at Sea

{Note: This section should define the bomb search procedure for when the ship is at sea. That procedure must reflect the specific staffing and arrangement of the ship, along with any security equipment (e.g., explosive vapor detectors)

17.3 EVACUATION OF THE SHIP

{Note: This section should define the responsibilities for calling for an evacuation of the ship and the procedure or conducting any required evacuation (to the extent a procedure can be defined in advance.)}

17.4 RESPONSE TO BREACH OF SECURITY OR TO SUSPICIOUS ACTIVITY ON, OR NEAR, THE SHIP

{Note: Awareness of suspicious activities and appropriate response to actual breaches of security are essential elements in a crew's readiness to prevent adverse security situations. This section should define the steps the ship's crew is to take if suspicious activities are noted or if a significant breach of security is recognized.}

17.5 SECURITY PROCEDURES WHILE IN DRYDOCK OR EXTENDED MAINTENANCE

{Note: This section should define the responsibilities within the company for maintaining the security of the ship while in dry-dock or extended maintenance situations (i.e., when a normal staffing situation does not apply). The focus should be on returning the ship to the crew and to normal service without any security vulnerabilities (e.g., hidden weapons, out-of-service security equipment, etc.)}

17.6 PROCEDURES AND SECURITY MEASURES WHEN SHIP IS AT A HIGHER SECURITY LEVEL THAN THE FACILITY

{Note: The company should define procedures and security measures the ship shall adopt if the ship is at a higher security level than the port.}

17.7 PROCEDURES AND SECURITY MEASURES WHEN SHIP IS AT PORT WHICH IS NOT A CONTRACTING GOVERNMENT

{Note: The company should establish procedures and security measures the ship should apply when it is at a port of State, which is not a Contracting Government, when it is interfacing with a ship to which this Code does not apply,it is interfacing with a fixed or floating platforms or a mobile drilling unit on location, or it is interfacing with a port or port facility which is not required to comply with chapter XI-2, Part A of the ISPS Code, or USCG regulation 33 CFR Subchapter H.}

SECTION 18

ADDITIONAL SHIP PROCEDURES

{Note: If this ship is a passenger ship, ferry, cruise ship, or on an international voyage, the company should address these additional security measures.}

18.1 PASSENGER SHIPS AND FERRIES

a. At all Security Levels, security sweeps are performed, prior to getting underway, after any period the ship was unattended.

b. At Security Level 2, in addition to Security Level 1 measures, the following security measures are implemented:

1. Searching selected areas prior to embarking passengers and prior to sailing

2. An alternative to the identification checks and passenger screening requirements in Section 6.3.b and Section 14 Table 6, the following security measures may be implemented:

i. Performing routine security patrols;

ii. Providing additional closed-circuit television to monitor passenger areas; or

iii. Securing all non-passenger areas.

{Note: Passenger ships certificated to carry more than 2000 passengers, working in coordination with the terminal, may be subject to additional vehicle screening requirements in accordance with a Security Directive or other orders issued by the Coast Guard.}

c. At Security Level 3, in addition to Security Levels 1 and 2 measures, as an alternative to the identification checks and passenger screening requirements in Section 6.3.b and Section 14 Table 6, ensure that random armed security patrols are conducted, which need not consist of ship personnel.

18.2 CRUISE SHIPS

a. At all Security Levels, the following security measures are addressed:

1. Screen all persons, baggage, and personal effects for dangerous substances and devices;

2. Check the identification of all persons seeking to board the ship; this check includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, government identification or visitor badges, or work orders;

3. Perform security patrols; and

4. Search selected areas prior to embarking passengers and prior to sailing.

b. At Security Level 3, security briefs are given about the specific threat are provided to passengers.

18.3 SHIPS ON INTERNATIONAL VOYAGE

a. ***{Note: An owner or operator of a U.S. flag ship, which is subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), must be in compliance with the applicable requirements of SOLAS Chapter XI–1, SOLAS Chapter XI–2and the ISPS Code, part A (Incorporated by reference, see § 101.115 of USCG Regulation 33 CFR Subchapter H).}***

b. ***{Note: Owners or operators of U.S. flag ships that are required to comply with SOLAS, must ensure an International Ship Security Certificate (ISSC) as provided in 46 CFR § 2.01–25 is obtained for the ship. This certificate must be issued by the Coast Guard.}***

c. ***{Note: Owners or operators of ships that require an ISSC in paragraph (b) of this section must request an inspection in writing, at least 30 days prior to the desired inspection date to the Officer in Charge, Marine Inspection for the Marine Inspection Office or Marine Safety Office of the port where the ship will be inspected to verify compliance with this part and applicable SOLAS requirements. The inspection must be completed and the initial ISSC must be issued prior to July 1, 2004.}***

SECTION 19

SHIP SECURITY ASSESSMENT

{Note: The ISPS Code requires that a copy of the Ship Security Assessment (SSA) be provided to the Flag Administration or RSO with the Ship Security Plan (SSP). The USCG requirement is that the SSA should be provided as part of the SSP. This location is where we suggest the SSA be provided, if it is considered part of the plan. Appendix 4 of the Guide describes an approach for performing the SSA.}