Shiptalk Security Guides

SHIPBOARD ACCESS CONTROL – What you need to know!

Steven Jones

Published by Shiptalk Publishing
Design Works
William Street
Gateshead
Tyne and Wear
NE10 0JP

Tel: +44 (0)191 4690877
Fax: +44 (0)191 4697940

Email: enquiries@shiptalkshop.com
Website: www.shiptalkshop.com

ISBN:
Edition 1 - Published 2007
Authors: Steven Jones

While this guide has been developed using the best information currently available, it is intended purely as guidance and is to be used at the user’s own risk. No responsibility is accepted by Shiptalk Ltd or by any person, firm, corporation or organization which has been in any way concerned with the furnishing of information or data, the compilation, publication or authorised translation, supply or sale of this guide, for the accuracy of any information or advice given herein or for any omission here from or for any consequences whatsoever resulting directly or indirectly from compliance with or adoption of guidance contained herein.

Abbreviations	
CSO	Company Security Officer
ID	Identification
ISPS Code	International Ship and Port Security Code
OOW	Officer Of The Watch
PFSO	Port Facility Security Officer
SSO	Ship Security Officer
SSP	Ship Security Plan

Introduction

The International Ship and Port Facility Security (ISPS) Code came into force on 1st July 2004, and amongst its many requirements is the demand that applicable vessels introduce measures to control access.

Access to the ship should be tightly controlled. The approved access route, in most cases the accommodation ladder, should be properly policed and only persons who have a proper reason should be allowed to board.

All persons boarding should be positively identified by an appropriate means of identification, which can be verified.

Unauthorised access routes should be guarded, for example by fitting guards on mooring ropes or anchor cables and ensuring that the deck and over-side areas are well lit. The deck areas should be patrolled regularly and the patrols should observe the approaches to the ship.

Since 2004 the US Coastguard has released figures regarding ship detentions for maritime security violations, consistently one of the most frequent reasons for a ship to have action taken against it was the issue of “Access Control”.

It is vital therefore that vessel personnel clamp down upon any weaknesses in their security in these regards.

The advice within this Shiptalk “What you need to know!” Security Guide provides an overview of some of the most common security practices that may form part of any maritime security regime with regards to basic access control and gangway entry management.

It is important to note that this is intended as guidance only and should not be considered to take precedence over the exact security requirements and procedures laid down within the Ship Security Plan (SSP), or the orders given by the Master, Company Security Officer (CSO), or Ship Security Officer (SSO).

Controlling Access

Why?

The ISPS Code requires that we:

- Prevent unauthorised persons gaining access
- Prevent unauthorised loading or discharge of goods/cargo
- Prevent the introduction of unauthorised weapons, incendiary devices, dangerous and illegal substances or explosives
- Control movement on, off and around vessel
- Prevent stowaways
- Deter attempted crime/terrorism
- Know who, what and when things come onboard
- Know who, what and when things leave

It is vital all know what to do, when and how. Items to be addressed should include

- Embarking/Disembarking procedures
- Communication procedures (internal and ship-to-shore),
- Logging

We need to control access to the vessel, and to ensure that ship security duties are performed properly.

It is also important to monitor deck areas, areas surrounding the ship as well as restricted areas onboard

We need to remember that handling of cargo and ships stores also have an effect on security, and when something goes wrong we need to have a reporting and communication system available.

So we know what has to be done, and then need to apply the rules with the normal common sense of good seamanship to make the vessel secure.

Where?

The gangway is the easiest point of access to a vessel when it is moored,

It is vital the gangway watch is given clear boarding procedures and when to call for assistance.

Remember the gangway is not the only place to watch, to control access we have to be aware of all potential means of access that we have to control and monitor:

- Access ladders
- Access gangways
- Access ramps
- Access doors, side scuttles, windows and ports
- Mooring lines and anchor chains
- Cranes and hoisting gear
- Rudder housings

We also have to control access, not just to the vessel but also to particular areas and equipment within the vessel.

Restricted areas to which access should be controlled include:

- Navigation bridge
- Machinery spaces and control spaces
- Security equipment control spaces
- Ventilation and Air Conditioning (A/C) systems/spaces
- Access to potable water tanks pumps/controls
- Other ship specific areas, as per SSP

Restricted property and equipment:

- Dangerous goods and hazardous substances
- Cargo pumps
- Cargo spaces
- Ships stores/essential maintenance equipment
- Navigation/communications equipment
- Medical equipment/stores

Access to vulnerable areas:

- Any key areas identified in the SSP, but not mentioned above
- Areas where unauthorised access could cause harm to people, vessel,
- equipment or cargo

Having fewer crew members can result in the gangway watch taking on additional responsibilities that require leaving the gangway unattended for periods of time. Make sure procedures exist to guard against this.

When?

Being secure is a permanent state – the level of threat can go up and down – but we must always treat security seriously, and do as we are instructed in the SSP.

Some vessels with apparently excellent daytime gangway security let down their guard after dark, but we need to ensure 24-hour coverage and vigilance.

Any security instructions need to make allowances for differing operations, and it is important that personnel are aware of the implications to security that are posed by each state, whether:

- At sea – full away, manoeuvring or pilotage
- Moored In port - working cargo, and silent periods
- At anchor,
- Alongside buoy moorings
- In dynamic positioning mode
- Not Under Command (NUC), or Restricted in Ability to Manoeuvre (RAM)
- In dry dock
- Ship-to-ship transfer
- Search and rescue
- Conducting exercises and drills

It is also vital to assess the effect of the tide on security. For instance a vessel with a low freeboard may become more susceptible to unauthorised entry when the tide drops to a certain level. It is important that the Officer of the Watch (OOW) and anyone else with security duties remain aware of the implications of such a change.

Who?

Onboard Security Responsibilities

The Master has overall responsibility for the Safety and Security of the Ship, the crew and cargo.

The SSO is responsible for implementing, maintaining and supervising all security procedures, training, drills, exercises and personnel assigned security duties onboard under the overall authority of the Master.

In most cases the OOW may be responsible for the following security related duties:

- Supervising security patrols and gangway watch
- Assisting gangway watch as required
- Processing visitors

Personnel with security duties are to do as instructed at all times, while all other personnel as a minimum must:

- Maintain security vigilance
- Challenge/question any unescorted person on board who is not a crew member
- Assist in the performance of vessel searches.
- Report deficiencies e.g. broken or missing locks, lights, etc, etc
- Ask questions if they are unsure

Who to grant access to?

It is important to stop those not allowed onboard, but to allow those who are.

The Master/SSO should instruct security watches with details of who is allowed access, and the things they need to provide in order to satisfy the security demands.

Such persons are likely to include:

- Shipboard personnel/staff
- Passengers
- Officials (Immigration, Port State Officers, Customs, Law Enforcement, Coastguard, port Health Officials)
- Company personnel (CSO, Superintendents, office staff)
- Operational visitors
- Bona fide visitors
- Supernumeraries
- Contractors/surveyors
- Agents
- Port officials (Port Facility Security Officer [PFSO], terminal managers, stevedores)

Who to deny access to?

The SSP will list the allowed criteria for entry to the vessel, and these may be supplemented with a list of expected people.

Mistakes will happen when trying to police access to the vessel – these mistakes need to err on the side of caution, it is far better to delay a legitimate visitor, and to ask for clarification of ID than it is to allow access to someone who should not be onboard.

In the event that someone gets rude or abusive the watchperson needs to call for immediate assistance from the SSO/OOW, and they will hopefully be able to calm the situation, and check the credentials of the person in question.

If someone has been denied access it is important to monitor their progress off the vessel – and the SSP should contain advice for escorting them from the vessel.

Access Control Options

Access Control can be done in four ways, physical, electronic, human, or procedural. A layered mix of these works best.

Physical barriers:

- Gangway
- Seals
- Doors, locks and keys
- Signage
- Fences

Such physical barriers are the most basic and common sense measures to deter, slow or stop unauthorised access onto or around the vessel.

The use of such equipment is fairly straightforward, and the measures should be positioned so as to work in conjunction with the other layers of security in place. Or can be used to push visitors into your next line of defence.

Just because the equipment is basic it still requires planning, foresight and training to position and use it in the most effective ways.

Locks for instance, need to be used properly – there are many ships that simply leave padlocks hanging down, or do not close doors. This needs to be addressed and all personnel with security duties should familiarise themselves with the measures in place, and keep a check that they are all used correctly.

Access Control Options

Electronic:

- Access Control Systems
- Closed Circuit TV (CCTV)
- Intruder Detection and Alarm Systems
- Lighting

The use of such advanced electronic systems can boost any security regime, but as with the physical measures they need to be used correctly.

Electronic access control and alarm systems need to be armed and operational. The investment in such equipment can be significant, and all personnel should be familiar with the operation and of any weaknesses.

CCTV systems can greatly aid the capability of personnel to monitor and protect large areas. However, it is important that cameras are sited correctly, that they work in harmony with other parts of the system (particularly lighting), and that they are monitored effectively.

Lighting can be a very strong deterrent to boarders – but again this must be used and fitted correctly. Avoid creating areas of shade, which can create hiding places for boarders. Also avoid blinding or dazzling security personnel and/or CCTV systems.

While these systems can aid security any over reliance can be detrimental, and should be guarded against. Use all means available to monitor security, and ensure that cross referencing of systems is done as routine.

Access Control Options

Human:

- Surveillance
- Patrolling
- Gangway, overside and deck watch

Shipboard personnel are vital to security, and they need to be:

- Fully briefed
- Knowledgeable about their instructions, and also
- Confident
- Trained and practised
- Supported by their seniors
- Familiar with any other security measures in place

The shipboard security regime is only as good as the people working within it. If the personnel are confident, if they understand their roles and responsibilities, and appreciate how important they are then the security will positively reflect this.

It is important that those charged with controlling the access to the vessel appreciate that they are the frontline of the vessel's security efforts, and they need to do all possible to ensure that they are up to this challenge.

Having people at the access point who look, sound and act with a reassuring confidence can have a major effect on the security of the vessel. Such people deter unauthorised boarders (they will simply move on to the next vessel) and they also act as a catalyst for security improvement around the whole vessel.

Security is no different to any other shipboard activity – if people are trained, skilled, enthusiastic and positive then they will achieve, and even exceed their aims.

Access Control Options

Procedural:

- Clear rules
- Checking of people
- What ID is acceptable
- When to deny access
- When to call the SSO/OOW

In order to harness the physical, electronic and human elements of security, and in order to demonstrate that the vessel is doing as required by the ISPS Code – it is important to lay down access control procedures.

These procedures will ensure that security assets are used properly and to best effect.

With adequate and effective procedures laid down security personnel should be fully aware of what they need to do, when they need to do it, and how it should be done.

In shipping it is no longer simply enough to do the “right thing”, we have to be able to document what was done – and so these procedures will then feedback into vital record keeping requirement for the vessel.

Main Access Point

The SSP should designate a “proper means of access”, this is usually a gangway/accommodation ladder, and whatever the security level in force should be the proper means of access to the vessel, and the focal point of access control measures.

The Gangway Watch reports to the SSO or the OOW and is responsible for:

- Deterring unauthorised entry
- Detecting unauthorised persons

One way to operate is the “SCAR” approach…

Stop
Check
Act (allow/deny access)
Record

On entry:

- Stop all persons attempting to gain access
- Check and authorise –ID, host, expected, listed, ID – Photos, validity, issuing authority
- Deny entry to unauthorised visitors
- Issue visitors pass to legitimate visitors, as per guidance in SSP
- Arrange escort
- Record details

On exit:

- Retrieve pass
- Record time of leaving

Main Access Point

This “proper means of access” area would benefit from being set up as a formal reception area,

The area should have clear external signing directing all visitors to this main entrance.

An entrance doorway should be designated by the SSP as its main entrance for the reception of visitors. The main entrance should be clearly marked and should be situated so that the watch person is the first point of contact for the visitor.

Ideally there will be some protection from the weather and an area for the watch person to process visitors.

The main entrance should ideally be a lockable door, which will only be opened when the watch person has deemed that access is permissible.

It may be advisable for there to be an alarm activation point, or permanent means of communication installed at this main entrance.

All other doors should carry signs stating, “No Admittance to unauthorised personnel”

Obviously many ships use alternate gangways, so it is advisable to replicate the reception areas on the port and starboard access points.

The Master and SSO should use their judgement to set up a security reception area which will work within the ship specific layout.

Main Access Point

The reception area should be clean and safe, and so personnel should perform some basic safety and “house keeping” checks alongside their security duties:

- Check the gangway is properly lashed and secure
- Check lighting
- Check safe for use
- Check persons boarding
- Check approaches to vessel
- Check for unauthorised boarding
- Check security signs in place

If something happens security personnel need to respond correctly, whether this is by reporting or requesting assistance.

Reporting:

- Recording details
- Use of radio/telephone

Calling for assistance:

- OOW
- SSO
- Master
- PFSO
- Law Enforcement Agents

The security watch person should know the order in which to call for assistance, and the circumstances under which to initiate an alarm. There should no be doubt or confusion in the watch persons mind, and they should be very clear on the benefits of prompt and decisive action.

Searching

One of the duties of the security watch may be to search persons, baggage, cargo or stores prior to them being afforded access to the vessel.

The SSP should state the circumstances under which searches will be initiated, and also the percentage of searches in relation to visitors, bags, etc. coming onboard.

There are some important issues to consider with such searching, and the SSO needs to ensure that the capabilities and support are properly applied.

Of immediate concern is the issue of resources, will the security watch be able to physically cope with the demands of searching while also managing access to the vessel? If there is any concern then additional resources may be necessary.

There is also the issue of training, and whether any hardware (such as metal detectors, vapour detectors, or x-ray scanners are used). It is vital that all personnel are trained in their use, and also understand any limitations in the systems used.

When searching it is may be necessary to implement policies for members of the opposite sex. Different rules may be necessary for different places and cultures – it is therefore important that the CSO, Master and SSO ensure that procedures are in place to manage such eventualities.

Visitor Logbooks

A Visitor Log should be maintained at the gangway.

The minimum details recorded in the log should include:

- Name
- Company
- ID Sighted and acceptable
- Person visited
- Date and Time of boarding
- Date and Time of leaving
- Visitor badge number issued

Keeping records is a vital part of the security process, and the importance of the visitor log should be stressed to all personnel.

The log should never, under any circumstances be falsified.

Basic Security Standing Orders

- The purpose of your duty is to maintain the security of the ship and prevent ANY person who is not in possession of a valid pass from gaining access to the ship.
- You are to check the passes of all persons coming on board and leaving the ship.
- Ensure that persons are in possession of valid identification.
- All visitors to the ship are to be issued with a visitor pass and required to sign for the pass BEFORE entering a restricted area. No unauthorised visitors are to be allowed access to the ship.
- Check that all ship personnel are in possession of an identification pass.
- You are to ensure that the passes of all persons (crew, contractors and visitors) are checked at the gangway when entering the ship.
- All people coming onboard are to pass through screening procedures when deployed.
- Depending on the Security Level applied at the time and in accordance with instructions issued by the SSO, hand baggage is to be searched as per procedures.
- You are to summon the assistance of the Duty Officer/SSO, using your VHF radio, if any person attempts to board the ship without identification.
- If during your watch any situation arises, which you consider requires the authority of an Officer, you are to politely request the visitor to wait at the gangway whilst you summon assistance on your VHF radio. Do not leave the person unattended.

In addition to these basic requirements it is vital to stress to the security watch person the vital role they play, and of the importance of awareness and vigilance in carrying out their duties.

Access Control and Security Levels: LEVEL 1

At security level 1, the security measures should include:

- Checking the identity of all persons seeking to board the ship and confirming a point of contact onboard

- In liaison with the port facility the ship should ensure that secure areas are established in which inspections and searching of people, baggage (including carry on items), personal effects can take place

- Segregating checked persons and their personal effects from unchecked persons and their personal effects

- Control of embarkation and disembarkation

- Identification of access points that should be secured or monitored to prevent unauthorised access

- Securing access to unattended spaces adjoining areas to which visitors have access; and

- Providing security briefings to all ship personnel on possible threats, reporting and the need for vigilance

- Searching those boarding as per SSP at Level 1

Access Control and Security Levels: LEVEL 2

As at Level 1, plus extra security measures to reflect the heightened risk to ensure higher vigilance and tighter control, include:

- Increasing the frequency of patrols around deck areas during night time hours to deter unauthorised access

- If necessary limit the number of access points to the ship, identifying those to be closed and the means of adequately securing them

- Where possible deter/prevent waterside access to the ship

- Encourage the PFSO to establish a restricted area on the shore-side of the ship, in close co-operation with the port facility

- Increasing the frequency and detail of searches of people, personal effects

- Escorting visitors whilst onboard the ship

- Providing additional specific security briefings to all ship personnel

- Carrying out a full or partial search of the ship

- Searching those boarding as per SSP at Level 2

Access Control and Security Levels: LEVEL 3

As at Level 1 and 2, plus the ship complies with the instructions issued by those responding to the security incident or threat thereof. Further additional security measures may include:

- The security measures taken by the ship, in close co-operation with those responding and the port facility include
- Additional resources guarding access control at the single, controlled, access point
- Granting access only to those responding to the security incident or threat
- More personnel readied to respond on board
- Suspension of embarkation or disembarkation
- If instructed the suspension of cargo handling operations, deliveries etc.
- Steps prepared for the evacuation of the ship
- Steps prepared for any necessary movement of the ship when instructed
- Preparing for a full or partial search of the ship if instructed
- Unless instructed otherwise provide a briefing to personnel informing them of the security status
- Searching those boarding as per SSP at Level 3, or by instruction from authorised parties

Training, Drills and Exercises

In order to properly prepare all those with access control duties it us vital to train them, and this can be done in a number of ways.

With gangway watch duties often the best approach is simple role playing – with other crewmembers taking on a range of different roles, some of whom should be granted access, others who should be denied, and also troublesome visitors for whom a greater degree of response may be necessary.

Range of exercises:

- Legitimate boarder
- Abusive boarder
- Law enforcement personnel
- Stevedores (with/without ID)
- PFSO
- Company Personnel (with/without ID)
- Female boarders (legitimate and none legitimate)

This should be done to not only train personnel, but also to give them the confidence to act properly, and to implement the SSP, It should also demonstrate to all who take part just how important their role is, and how responsible they are for the security of the vessel.

Third Party Guards

In some ports, ships are regularly and routinely required to use additional protective shorebased security.

It is important that the CSO is made aware of this and can undertake dialogue with the PFSO if necessary, it is also vital the SSO understands the exact security role performed by these external guards.

The SSO must know which areas of the vessel they will cover, and also the main focus of the security, whether they there to stop people accessing the vessel, or as is the case in some ports, whether they are purely looking to ensure that seafarers do not leave.

Risk Management and Planning

In order to ensure the most effective access controls, it is important to consider the place/port/anchorage that the vessel will be visiting.

The CSO, Master and SSO should be aware of the threats most likely to be encountered and should gear the vessel's defences accordingly.

In order to best secure access to the vessel personnel should be fully briefed as to the threats facing them and the vessel, and be given support and instruction on how best to guard against attack.

Is there a history at the port of?

- Stowaways
- Pilferage
- Piracy
- Drug smuggling
- Terrorism
- Prostitution
- Kidnappings
- Vandalism
- Protests
- Fraud
- Racketeering

It is no point in having the security assets and resources geared up for non-existent or unlikely threats – so we need to look forward and plan effectively. Failure to properly plan for known threats undermines the shipboard security regime and can waste the time and efforts of all involved.

Security personnel should also be encouraged to ask questions and to keep themselves abreast of the threats which they are most likely to be exposed to.

The ISPS Code is very much a "risk management" tool, and therefore this is a vital stage of the security process.

Port Security

For all of the security measures onboard a vessel, effective security in port is only possible if the port authority and terminal operator also engage in effective security measures.

Items to consider for port security include:

- Guarding the perimeter of the terminal
- Access and egress of only legitimate traffic
- Internal monitoring of movement
- Surveillance and protection of the water borne boundaries
- Control and monitoring of stevedores and others working inside the port
- Regular drills for bomb threats, hostage situations and intruders and practicing security measures in all terminal employees' routines

Port procedures and plans should be communicated to calling vessels and coordinated with vessel procedures and requirements. For example, security plans should be raised and coordinated during the initial operations briefing held between the vessel's cargo officer and the load/discharge supervisor ashore.

Ideally, operations checklists provided by each party in this meeting should reflect security requirements.

Additionally port authorities must effectively coordinate all elements of the system (i.e. working with shipping agents to gain access to cargo manifests, ETA, ETD, previous port of call, destination and tracking movements of dangerous materials/cargoes in the port).

The ship and port need to work together to ensure security – but no vessel should ever rely on the port. Security is your business!

About the Author

Having been attacked by pirates when serving as a deck officer, Steven Jones has long had an interest and involvement in maritime security issues. This led to his attendance at the IMO during the sessions leading to the adoption of the ISPS Code, and consequently Steven has advised numerous shipping companies on their security planning.

Having worked in marine fraud investigations and as a security specialist at a major protection and Indemnity association he then took his years of research, professional involvement and in-depth knowledge of the ISPS Code to produce the book, “Maritime Security”, published by The Nautical Institute.

Steven currently provides security comment and assessment for a number of maritime publications, he is a member of the advisory panel for the Leicester University Maritime and Supply Chain Security Diploma, a regular speaker at numerous Conferences and has guest lectured on a number of University and college courses.