Clear Form

USCG Marine Safety Center/Vessel Securty Division

Vessel Security Plan Stage II Checklist

Company Name:	**Case:**	**Date:**
Vessel Name(s)/ O.N.:		**Revised:**
Foreign Flagged: No **Vessel Class/Type:**	**Int'l Travel:**	**Tonnage:**

Reviewer:	**Compliance**			
QA:	**YES**	**NO**	**N/A**	**Comments**
49 C.F.R. § 1520.13 Marking SSI				
2.a) The SSI marking consisting of the words "SENSITIVE SECURITY INFORMATION" must be applied to the header of each page of the security plan.	☐	☐	☐	
2.b) The following statement must be applied to the footer of each page: "WARNING: This record contains Sensitive Security Information that is controlled under the provisions of 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a 'need to know', as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520."	☐	☐	☐	
104.305 Vessel Security Assessment (VSA) Requirements				
d) VSA Report.				
1) Vessel Owner/Operator must ensure that a written VSA Report is prepared and included as part of the VSP. The VSA Report must contain:				
i) A summary of how the on-scene survey was conducted;		☐	☐	
ii) Existing security measures, procedures and operations;		☐	☐	
iii) A description of each vulnerability found during the assessment;		☐	☐	
iv) A description of security countermeasures that could be used to address each vulnerability;		☐	☐	
v) A list of the key vessel operations that are important to protect;		☐	☐	
vi) The likelihood of threats to key vessel operations; and		☐	☐	
vii) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the vessel.		☐	☐	
2) The VSA Report must address the following elements onboard or within the vessel:				
i) Physical security;		☐	☐	
ii) Structural integrity;		☐	☐	
iii) Personnel protection systems;		☐	☐	
iv) Procedural policies;		☐	☐	
v) Radio and telecommunication systems, including computer systems and networks and;		☐	☐	
vi) The other areas that may, if damaged or used illicitly, pose a risk to people, property or operations onboard the vessel or within a facility.		☐	☐	
3) The VSA Report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:				
i) Vessel personnel;		☐	☐	
ii) Passengers, visitors, vendors, repair technicians, facility personnel, etc.;		☐	☐	
iii) Capacity to maintain safe navigation and emergency response;		☐	☐	
iv) Cargo, particularly dangerous goods and hazardous substances;		☐	☐	
v) Vessel stores;		☐	☐	
vi) Any vessel security communication and surveillance systems; and		☐	☐	

vii) Any other vessel security systems, if any;				
4) The VSA Report must account for any vulnerabilities in the following areas;				
i) Conflicts between safety and security measures;				
ii) Conflicts between vessel duties and security assignments;				
iii) The impact of watch keeping duties and risk of fatigue on vessel personnel alertness and performance;				
iv) Security training deficiencies; and				
v) Security equipment and systems, including communication systems.				
5) The VSA Report must discuss and evaluate key vessel measures and operations, including:				
i) Ensuring performance of all security duties;				
ii) Controlling access to the vessel, through the use of identification systems or otherwise;				
iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);				
iv) Supervising the handling of cargo and the delivery of vessel stores;				
v) Monitoring restricted areas to ensure that only authorized persons have access;				
vi) Monitoring deck areas and areas surrounding the vessel; and				
vii) The ready availability of security communications, information, and equipment.				
e) The VSA must be documented and the VSA Report retained by the vessel owner or operator with the VSP. The VSA, the VSA Report and VSP must be protected from unauthorized access or disclosure.				
Vessel Details and Company Contact Information to Include:				
Vessel or Multiple Vessel Specifics. List page:				
Vessel Schematic for Designated Passenger/Employee Access Areas				
Company Address				
Company Phone Number				
CSO Mailing and E-mail Address				
104.205 Master				
a) Authority of Master to make decision to maintain the safety and security of the vessel.				
b) If there is a conflict between safety and security, Master can take action to best maintain the safety of the vessel. In such cases:				
1) The Master must notify the Captain of the Port (COTP).				
2) Security measures must be commensurate with the prevailing MARSEC Level.				
3) Owner/operator must ensure that conflicts are resolved to the satisfaction of the COTP, or the Commandant for vessels on international voyages and that recurrence is minimized.				
104.210 Company Security Officer (CSO)				
a) General				
1) Owner/Operator must designate a CSO in writing.				
2) If more than one CSO, each must be designated ships for which responsible.				
3) CSO may be assigned other duties including those of VSO, provided he/she able to perform those required of CSO.				
4) If the CSO delegates duties, VSP must contain wording saying that the CSO remains responsible for the performance of those duties.				
5) The CSO must maintain a TWIC.				

b) Qualifications.							
1) CSO must have general knowledge through training or equivalent experience in the following:	CSO	VSO	CSO	VSO	CSO	VSO	
i) Security administration and organization of company's vessels;			■	■	■	■	
ii) Vessel, facility and port operations relevant to that industry;			■	■	■	■	
iii) Vessel and facility security measures, requirements at the different MARSEC Levels;			■	■	■	■	
iv) Emergency preparedness and response and contingency planning;			■	■	■	■	
v) Security equipment and systems;			■	■	■	■	
vi) Methods of conducting audits, and techniques for inspecting, controlling, and monitoring techniques; and			■	■	■	■	
vii) Techniques for security training and education, including security measures/procedures.			■	■	■	■	
2) Relevant requirements in Part 104.210 (b)(2)							
i) Relevant international conventions, codes, and recommendations;			■	■	■	■	
ii) Relevant government legislation and regulations;			■	■	■	■	
iii) Responsibilities and functions of other security organizations;			■	■	■	■	
iv) Methodology of Vessel Security Assessment;			■	■	■	■	
v) Methods of vessel security surveys and inspections;			■	■	■	■	
vi) Instruction techniques for security training and education, including security measures and procedures;			■	■	■	■	
vii) Handling sensitive security information and security related communications;			■	■	■	■	
viii) Knowledge of current security threats and patterns			■	■	■	■	
ix) Recognition and detection of dangerous substances and devices;			■	■	■	■	
x) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;			■	■	■	■	
xi) Techniques used to circumvent security measures;			■	■	■	■	
xii) Methods of physical screening and non-intrusive inspections;			■	■	■	■	
xiii) Security drills and exercises, including drills and exercises with facilities; and			■	■	■	■	
xiv) Assessment of security drills and exercises; and			■	■	■	■	
xv) Knowledge of TWIC requirements.				■		■	
c) Responsibilities							
In addition to duties specified elsewhere, the CSO for each vessel must:							
1) Keep vessel apprised of potential threats;				■		■	
2) Ensure a Vessel Security Assessment is carried out;				■		■	
3) Ensure a Vessel Security Plan (VSP) is developed, approved and maintained;				■		■	
4) Ensure the VSP is modified when necessary;				■		■	
5) Ensure the vessel's security activities are audited;				■		■	
6) Arrange for Coast Guard inspections under 46 CFR Part 2;				■		■	
7) Ensure timely correction of problems identified by audits;				■		■	
8) Enhance awareness and vigilance within the ship-owners organization;				■		■	
9) Ensure personnel receive adequate security training;				■		■	
10) Ensure communication/cooperation with vessel, facility, and/or port;				■		■	
11) Ensure consistency between security requirements and safety requirements;				■		■	
12) Ensure that vessel specific information is included when several similar types vessel plans are submitted;				■		■	
13) Ensure compliance with Alternative Security Plan (ASP) or equivalent, if appropriate, and				■		■	
14) Ensure security measures give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods				■		■	

15) Ensure the TWIC program is being properly implemented.				
104.215 Vessel Security Officer (VSO)				
a) General				
1) VSO may be assigned other duties provided he/she able to perform those required of VSO.				
2) For manned vessels, the VSO must be the Master or a member of the crew and the VSP must identify how the VSO can be contacted.				
3) For unmanned vessels the VSO must be a company employee and may serve as VSO for more than one unmanned vessel. If serving as VSO for more than one unmanned vessel, list of vessels for which responsible must be in the VSP.				
4) The VSO of any unmanned barge and the VSO of any interfacing towing vessel must coordinate/implement security measures for interfacing period.				
5) If the VSO delegate duties, VSP must contain wording saying that the VSO remains responsible for the performance of those duties.				
6) The VSO must maintain a TWIC.				
b) Qualifications				
VSO must have knowledge through training or equivalent job experience in the following:				
1) The same CSO qualifications listed in 33 CFR 104.210 (b)(1) & (2);				
2) Vessel layout;				
3) The VSP and related procedures including scenario-based response training;				
4) Crowd management and control techniques;				
5) Operations of security equipment and systems;				
6) Testing and calibration of security equipment and systems, and their maintenance at sea; and.				
7) TWIC.				
c) Responsibilities				
In addition to the duties and responsibilities mentioned elsewhere, the VSO must perform the following:				
1) Regularly inspect the vessel to ensure security measures are maintained;				
2) Ensure maintenance and supervision of implementation of the VSP and amendments;				
3) Ensure coordination of handling cargo, vessel stores and bunkers in compliance with rule;				
4) Propose modifications to the VSP to the CSO;				
5) Ensure any problems during audits/inspections are reported to the CSO and implement;				
6) Ensure security awareness and vigilance onboard the vessel;				
7) Ensure adequate training for the vessel personnel;				
8) Ensure the reporting and recording of all security incidents;				
9) Ensure the coordination/implementation of the VSP with the CSO and Facility Security Officer (FSO) when applicable;				
10) Ensure security equipment is properly operated, tested, calibrated, and maintained; and				
11) Ensure consistency between security requirements and proper treatment of crew.				
12) VSO ensures TWIC programs are in place and implemented appropriately.				

104.220 Company or Vessel Personnel with Security Duties				
Company and vessel personnel responsible for security duties must maintain a TWIC; and				
must have knowledge, through training or equivalent job experience, in the following,				
a) Knowledge of current security threats and patterns;				
b) Recognition and detection of dangerous substances and devices;				
c) Recognition of characteristics/behavioral patterns of those 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, calibration and maintenance of security systems while at sea;				
j) Inspection, control and monitoring techniques;				
k) Relevant provisions of the security plan;				
l) Methods of physical screening of persons/personal effects baggage cargo/vessels stores; and				
m) The meaning and requirements of each MARSEC Level.				
n) Relevant aspects of the TWIC program and how to carry them out.				
104.225 Security Training for all Other Vessel Personnel.				
All other vessel personnel, including contractors, whether part-time, full-time, temporary, or permanent, <u>must</u> have knowledge of, through training or equivalent job experience in the following, as appropriate:				
a) Relevant provisions of the VSP;				
b) The consequential requirements of the different MARSEC Levels;				
c) Recognition and detection of dangerous substances and devices;				
d) Recognition and characteristics/behavioral patterns of those likely to threaten security; and				
e) Techniques used to circumvent security measures.				
f) Relevant aspects of the TWIC program and how to carry them out.				
104.230 Drill and Exercise Requirements.				
a) General				
1) Drills and exercises test the proficiency of the crew at different MARSEC Levels and implement VSP. They must enable VSO to identify any related security deficiencies needed to be addressed.				
2) Drills and exercises may be satisfied by actual MARSEC increase provided attainment is reported to the COTP.				
b) Drills.				
1) VSO must ensure that at least one security drill is conducted at least once every 3 months.				
2) Drills must test individual elements of the VSP including response to threats/incidents.				
3) Vessels may participate in a facility's scheduled drill.				
4) Drill must be conducted within one week from when crew without drill experience on that vessel exceeds 25%.				
c) Exercises.				
1) Exercises must be conducted each calendar year with no more than 18 months between exercises.				
2) Exercises may be: (exercise format must satisfy at least one of the following for "Yes")				
i) Full scale or live;				

ii) Tabletop simulation or seminar;				
iii) Combined with other appropriate exercises; or				
iv) A combination of elements in paragraphs (c) (2) (i) through (iii) of this section.				
3) Exercises may be vessel specific or cooperative to incorporate facility/vessel/port exercises.				
4) Each exercise must test communication / notification / coordination / resources & response.				
5) Exercises are a full test of security program, must include relevant company and vessel security personnel and may include facility and/or government resources depending on scope & nature of exercises.				
104.235 Vessel Recordkeeping Requirements.				
a) The VSO must keep records of activities in paragraph (b) of this section for at least 2 years unless otherwise stated and made available to the Coast Guard upon request.				
b) Records required by this section MAY be kept in electronic format but if so, they MUST be specifically protected.				
The following records must be kept:				
1) Training (2 years);				
2) Drills and exercises (2 years);				
3) Incidents and breaches of security (2 years);				
4) Changes in MARSEC Levels (2years);				
5) Maintenance, calibration and testing of security equipment (2 years);				
6) Security threats (2 years);				
7) Declaration(s) of security (for one-time DoS', keep the last 10; for continuing DoS', keep at least 90 days after the expiration date)				
8) Annual audit of the VSP (2 years);				
c) Any records required by this part must be protected from unauthorized access or disclosure.				
104.240 MARSEC Level Coordination and Implementation.				
a) Owner/Operator must ensure prior entering port or visiting an OCS facility, all measures taken as in VSP for compliance with MARSEC Level in effect in that port/facility.				
b) **When notified of increase in MARSEC Level, vessel Owner Operator must ensure the following**:				
1) If higher MARSEC Level set for port which vessel is in or about to enter, vessel complies **without undue delay** with all measures specified in VSP for compliance with that higher MARSEC Level;				
2) The COTP is notified as required by 33 CFR 101.300 (c) when compliance with higher MARSEC Level is implemented;				
3) For vessels in port that compliance with higher level has taken place **within 12 hours** of notification, and				
4) If higher MARSEC Level set for OCS facility to be visited, the vessel complies without delay, with all measures specified in the VSP for compliance with that higher MARSEC Level.				
c) **For MARSEC Levels 2 and 3**, VSO must brief crew of threats/reporting procedures, and stress need for high vigilance.				
d) Owner/Operator whose vessel is not in compliance with requirements in this section must inform COTP to obtain approval prior to entering any port, to interfacing with another vessel or facility, or to continuing operations.				
e) **For MARSEC Level 3**, Owner/Operator may be required to implement additional measures that ***may include*** the following:				
1) Arrangements to ensure that vessel can be towed or moved if deemed necessary by USCG;				
2) Use of waterborne security patrol;				

3) Use of armed security personnel to control access to vessel and to deter a security incident; or				
4) Screening the vessel for presence of dangerous substances and devices underwater or other threats.				
104.245 Communications				
a) The VSO must have a means to effectively notify crew of changes in security conditions onboard vessel.				
b) Communication systems and procedures must allow effective and continuous communication between vessel security personnel, interfacing facilities/vessels and national or local authorities with security responsibilities.				
c) Communication systems and procedures must enable vessel personnel to notify shore side authorities or other vessels of a security threat or incident onboard in a timely manner.				
104.250 Procedures for Interfacing with Facilities and Other Vessels.				
a) Vessel Owner/Operator must ensure interface measures with other vessels/facilities at all MARSEC Levels.				
b) For each U.S. flag vessel calling foreign ports/facilities, owner/operator must ensure procedures for interfacing w/same are established.				
104.255 Declaration of Security (DoS)				
a) Each vessel must have procedures for requesting DoS and handling DoS requests from facility or other vessel.				
b) **At MARSEC Level 1**, cruise ships, or manned vessels carrying Certain Dangerous Cargoes (CDC) in bulk, must complete DoS with VSO or Facility Security Officer (FSO) of interfacing vessel/facility.				
1) For vessel-to-facility interface, prior to cargo transfer/passengers FSO or Master, VSO or designee must agree on and sign DoS.				
2) For vessel-to-vessel interface, prior to cargo transfer/passengers VSO's must agree on and sign DoS.				
c) **At MARSEC Levels 2 and 3**, respective Master/VSO/designee for manned vessel before vessel-to-vessel interface and prior to passenger/cargo transfer must sign DoS.				
d) **At MARSEC Levels 2 and 3**, respective Master/VSO/designee for manned vessel must agree on DoS before vessel-to-facility interface and sign DoS before passenger/cargo transfer.				
e) At MARSEC Levels 1 and 2, VSO of vessel that frequently calls same facility, may implement continuous DoS provided:				
1) The DoS is valid for the specific MARSEC Level;				
2) The effective period at MARSEC Level 1 does not exceed 90 days; and				
3) The effective period at MARSEC Level 2 does not exceed 30 days.				
f) When MARSEC Level increases beyond level in DoS, continuing DoS is void and a new one required.				
g) COTP may require at anytime at any MARSEC Level any manned vessel to implement DoS with VSO/FSO prior to vessel-to-vessel activity or vessel-to-facility interface when deemed necessary.				
101.505 Declaration of Security (DoS) (104.255)				
A sample DoS Form must be provided with VSP.				
104.260 Security Systems and Equipment Maintenance				
a) Security systems/equipment to be in good order and tested calibrated maintained according to manufacturer's recommendations.				
b) Results of tests as per paragraph (a) to be recorded in accord with 33 CFR 104.235. Deficiencies to be promptly corrected.				
c) VSP must include procedures for identifying and responding to security equipment failures/malfunctions.				

104.265 Security Measures for Access Control.				
a) General - Vessel Owner/Operator must ensure implementation of security measures to:				
1) Deter unauthorized introduction of dangerous substances or devices;				
2) Secure dangerous substances that are authorized by the owner to be onboard; and				
3) Control access to the vessel;				
4) Prevent an unescorted individual from entering an area of the vessel that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.				
b) The vessel owner or operator must ensure the following are specified:				
1) The locations providing means of access to the vessel where access restrictions or prohibitions are applied for each Maritime Security (MARSEC) Level, including those points where TWIC access control provisions will be applied. "Means of access" include, but are not limited, to all:				
i) Access ladders;				
ii) Access gangways;				
iii) Access ramps;				
iv) Access doors, side scuttles, windows and ports;				
v) Mooring lines and anchor chains; and				
vi) Cranes and hoisting gear.				
2) The types of restriction to be applied and the means of enforcing them; and				
3) The means used to establish the identity of individuals not in possession of a TWIC and procedures for escorting, in accordance with 101.515 of this subchapter; and				
4) Procedures for identifying authorized and unauthorized persons at any MARSEC Level.				
c) The vessel owner or operator must ensure that a TWIC program is implemented as follows:				
1) **All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with §101.514 of this subchapter. Inspection must include**:				
i) A match of the photo on the TWIC to the individual presenting the TWIC;				
ii) Verification that the TWIC has not expired; and				
iii) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.				
2) If an individual cannot present a TWIC because it has been lost, damaged or stolen, and he or she has previously been granted unescorted access to the vessel and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than seven consecutive calendar days provided that:				
i) The individual has reported the TWIC as lost, damaged, or stolen to TSA as required in 49 CFR 1572.19(f);				
ii) The individual can present another identification credential that meets the requirements of 33 CFR 101.515; and				
iii) There are no other suspicious circumstances associated with the individual's claim of loss or theft.				

3) If an individual cannot present his or her TWIC for any other reason than outlined in paragraph (2) of this section, he or she may not be granted unescorted access to the secure area. The individual must be under escort, as that term is defined in 33 CFR 101, at all times when inside a secure area.				
4) With the exception of persons granted access according to paragraph (2) of this section, all persons granted unescorted access to secure areas of the vessel must be able to produce his or her TWIC upon request.				
5) There must be disciplinary measures in place to prevent fraud and abuse.				
6) The vessel's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of facilities or other transportation conveyances that interface with the vessel.				
d) If the vessel owner or operator uses a separate identification system, ensure that it complies and is coordinated with TWIC provisions in this part.				
e) The vessel owner or operator must establish in the approved VSP the frequency of application of any security measures for access control, particularly if these security measures are applied on a random or occasional basis.				
f) MARSEC Level 1 - Owner/Operator must ensure that the security measures in this paragraph are implemented to:				
1) Employ TWIC as set out in paragraph (c) of this section.				
2) Screen persons, baggage (including carry-on items), personal effects, and vehicles for dangerous substances and devices at the rate specified in the approved VSP, except for government-owned vehicles on official business when government personnel present identification credentials for entry;				
3) Conspicuously post signs that describe security measures currently in effect and clearly state that:				
i) Boarding the vessel is deemed valid consent to screening or inspections; and				
ii) Failure to consent to screening/inspection will result in denial or revocation of authorization to board.				
4) Check the identification of any person not holding a TWIC and seeking to board the vessel, including vessel passengers, vendors, personnel duly authorized by the cognizant government authorities, and visitors. This check includes confirming the reason for boarding by examining at least one of the following:				
i) Joining instructions;				
ii) Passenger tickets;				
iii) Boarding passes;				
iv) Work orders, pilot orders, or survey of orders;				
v) Government identification; or				
vi) Visitor badges issued in accordance with an identification system implemented under paragraph (d) of this section.				
5) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of vessel personnel or a law enforcement officer, to establish his or her identity in accordance with this part or to account for his or her presence on board. Any such incident must be reported in compliance with this part;				
6) Deny unauthorized access to the vessel;				
7) Identify access that must be secured or attended to deter unauthorized access;				
8) Lock or prevent access to unattended spaces that adjoin areas to which passengers/visitors have access;				

9) Provide a designated area on board, within the secure area, or in liaison with a facility, for conducting inspections and screening of people, baggage (including carry-on items), personal effects, vehicles and the vehicle's contents;				
10) Ensure vessel personnel are not subjected to screening, of the person or of personal effects, by other vessel personnel, unless security clearly requires it;				
11) Conduct screening in a way that takes into full account individual human rights and preserves the individual's basic human dignity;				
12) Ensure the screening of all unaccompanied baggage;				
13) Ensure checked persons and their personal effects are segregated from unchecked persons and their personal effects;				
14) Ensure embarking passengers are segregated from disembarking passengers;				
15) Ensure, in liaison with the facility, a defined percentage of vehicles to be loaded aboard passenger vessels are screened prior to loading at the rate specified in the approved VSP;				
16) Ensure, in liaison with the facility, all unaccompanied vehicles to be loaded on passenger vessels are screened prior to loading; and				
17) Respond to the presence of unauthorized persons onboard, including repelling unauthorized boarders.				
g) MARSEC Level 2 - In addition to measures taken at Level 1, The additional security measures required ***may include*** the following:				
1) Increasing the frequency and detail of screening people/personal effects/vehicles being embarked, except for gov't-owned vehicles on official business with proper credentials for entry;				
2) X-ray screening of all unaccompanied baggage;				
3) Assigning additional personnel to patrol decks during periods of reduced vessel operations;				
4) Limiting the number of access points to the vessel by closing and securing some;				
5) Denying access to visitors who do not have a verified destination;				
6) Deterring waterside access to the vessel which may include the facility providing boat patrols; and				
7) Establishing a restricted area on the shore side of the vessel in cooperation with the facility.				
h) MARSEC Level 3 - In addition to measures taken at Level 1 and Level 2, The additional security measures required ***may include*** the following:				
1) Screening all persons, baggage and personal effects for dangerous substances and devices;				
2) Performing one or more of the following on unaccompanied baggage:				
i) Screen unaccompanied baggage more aggressively, for example, X-ray from two or more angles;				
ii) Prepare to restrict or suspend handling unaccompanied baggage; or				
iii) Refuse to accept unaccompanied baggage onboard;				
3) Being prepared to cooperate with responders and facilities;				
4) Limiting access to the vessel to a single controlled access point;				
5) Granting access to only those responding to the security incident or threat;				
6) Suspending embarkation or disembarkation of personnel;				
7) Suspending cargo operations;				
8) Evacuating the vessel;				
9) Moving the vessel; and				
10) Preparing for a full or partial search of the vessel.				

104.267 Security measures for newly hired employees.				
a) Newly-hired vessel employees may be granted entry to secure areas of the vessel for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements in paragraph (b) of this section are met, and provided that the new hire is accompanied by an individual with a TWIC while within the secure areas of the vessel. If TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend access to secure areas for another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. The Coast Guard will issue guidance for use in making these determinations.				
b) Newly-hired vessel employees may be granted the access provided for in paragraph (a) of this section only if:				
1) The new hire has applied for a TWIC in accordance with 49 CFR Part 1572 by completing the full enrollment process, paying the user fee, and is not currently engaged in a waiver or appeal process. The vessel owner or operator or Vessel Security Officer (VSO) must have the new hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC;				
2) The vessel owner or operator or the VSO enters the following information on the new hire into the Coast Guard's Homeport website (*http://homeport.uscg.mil*):				
i) Full legal name, including middle name if one exists;				
ii) Date of birth;				
iii) Social security number (optional);				
iv) Employer name and 24 hour contact information; and				
v) Date of TWIC enrollment;				
3) The new hire presents an identification credential that meets the requirements of §101.515 of this subchapter;				
4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the vessel owner or operator or VSO have not been informed by the cognizant COTP that the new hire poses a security threat; and				
5) There would be an adverse impact to vessel operations if the new hire is not allowed access.				
c) This section does not apply to any individual being hired as a Company Security Officer (CSO) or VSO, or any individual being hired to perform vessel security duties.				
d) The new hire may not begin working on board the vessel under the provisions of this section until the owner, operator, or VSO receives notification, via Homeport or some other means; the new hire has passed an initial name check.				
104.145 MARSEC Directives (Performance Standards)				
Owner/operator must have procedures to verify screening rates described in the VSP. Rates may be measured over a reasonable time period determined by the CSO/VSO. The period should be noted in the VSP. Minimum rates for each MARSEC Level should be per the tables provided in appropriate Directive below, as applicable:				
104-1 Cruise Ship				
104-2 Passenger Vessel/Ferry				
104-3 Cargo/Towing/Other Commercial Vessel				
104-4 MODU/OSV Vessel				
104-5 Passenger Vessel/Ferry Performance Standards				

104.270 Security Measures for Restricted Areas				
a) General - The Owner/Operator must ensure the designation of restricted areas in order to:				
1) Prevent or deter unauthorized access;				
2) Protect persons authorized to be onboard;				
3) Protect the vessel;				
4) Protect sensitive security areas within the vessel;				
5) Protect security and surveillance equipment and systems; and				
6) Protect cargo and vessel stores from tampering.				
b) Designation of restricted areas. Owner/Operator must ensure restricted areas are designated as specified in the approved VSP. Restricted areas must include, as appropriate:				
1) Navigation bridge, machinery spaces, and other control spaces;				
2) Spaces containing security and surveillance equipment, and their controls and lighting system controls;				
3) Ventilation and A/C systems, and other similar spaces;				
4) Spaces with access to potable water tanks, pumps or manifolds;				
5) Spaces containing dangerous goods or hazardous substances;				
6) Spaces containing cargo pumps and their controls;				
7) Cargo spaces and spaces containing vessels stores;				
8) Crew accommodations; and				
9) Any other spaces or areas vital to the security of the vessel.				
c) Owner/Operator must ensure that measures and policies are established to:				
1) Identify which vessel personnel are authorized to have access;				
2) Determine which persons other than vessel personnel are authorized to have access;				
3) Determine the conditions under which that access may take place;				
4) Define the extent of any restricted area;				
5) Define the times when access restrictions apply; and				
6) Clearly mark all restricted areas and that unauthorized presence constitutes a breach of security.				
d) **MARSEC Level 1** - Owner/Operator must ensure security measures to prevent unauthorized access. Security measures ***may include*****:**				
1) Locking or securing access points;				
2) Monitoring or using surveillance equipment;				
3) Using guards or patrols; and				
4) Using automatic intrusion devices to activate audible/visual alarm at a location continuously attended or monitored to alert vessel personnel to unauthorized access.				
e) **MARSEC Level 2** - In addition to measures taken at Level 1, additional measures ***may include*** the following:				
1) Increasing the frequency and intensity of monitoring and access controls on existing restricted access areas;				
2) Restricting access to areas adjacent to access points;				
3) Providing continuous monitoring of each area, using surveillance equipment; and				
4) Dedicating additional personnel to guard or patrol each area.				
f) **MARSEC Level 3** - In addition to measures taken at Levels 1 and 2, additional measures ***may include*** the following:				
1) Restricting access to additional areas; and				
2) Searching restricted areas as part of a security sweep of the vessel.				

104.275 Security Measures for Handling Cargo.				
a) **General - Owner/Operator must ensure security measures related to cargo handling are specified in order to:**				
1) Deter tampering;				
2) Prevent cargo not meant for carriage from being accepted and stored on the vessel;				
3) Identify cargo that is approved for loading onto the vessel;				
4) Include inventory control procedures at access points to the vessel; and				
5) When there are regular/repeated cargo ops with same shipper, coordinate security measures with the shipper/responsible party in accordance with established agreement and procedures.				
b) MARSEC Level 1 - Owner/Operator must ensure the implementation of measures to:				
1) Unless unsafe to do so; routinely check cargo and cargo spaces prior to and during cargo handling for evidence of tampering;				
2) Check that cargo to be loaded matches the cargo documentation or container numbers match shipping documents;				
3) Ensure in liaison with facility, that vehicles loaded on RO-RO and passenger ships are screened before loading as per frequency specified in VSP; and				
4) Check seals or other methods used to prevent tampering. Liaison with facility, if necessary.				
c) **MARSEC Level 2** - Owner/Operator to ensure implementation of additional security measures which ***may include*** the following:				
1) Increase the frequency and detail of checking cargo and cargo spaces for evidence of tampering;				
2) Intensify checks to ensure that only intended cargo/containers or other units are loaded;				
3) Intensify screening of vehicles to be loaded on RO-RO and passenger vessels;				
4) In liaison with facility, increasing frequency and detail in checking seals and other methods to prevent tampering;				
5) Increasing frequency and intensity of visual and physical inspections; or				
6) Coordinating enhanced security measures with the shipper or other party i/a/w established agreement and procedures.				
d) **MARSEC Level 3** - In addition to measures at Level 1 and 2, additional measures which ***may include:***				
1) Suspending loading or unloading of cargo;				
2) Being prepared to cooperate with responders, facilities, and other vessels; or				
3) Verifying the inventory and location of any hazardous materials carried on board.				
104.280 Security Measures for Delivery of Vessel Stores and Bunkers				
a) General - Owner/Operator must ensure security measures for delivery of stores/bunkers are implemented to:				
1) Check vessel stores for package integrity;				
2) Prevent vessel stores from being accepted without inspection;				
3) Deter tampering; and				
4) Prevent vessel stores and bunkers from being accepted unless ordered.				
b) MARSEC Level 1 - Owner/Operator must ensure the implementation of measures to:				
1) Check vessel stores before being accepted;				

2) Check that stores and bunkers match the order prior to being brought onboard or bunkered; and				
3) Ensure stores are controlled or immediately and securely stowed following delivery.				
c) **MARSEC Level 2** - In addition to measures taken at Level 1, additional security measures ***may include:***				
1) Intensify the inspection of vessel stores during delivery; or				
2) Checking vessel stores prior to receiving them onboard.				
d) **MARSEC Level 3** - In addition to security measures at Levels 1and 2, additional security measures ***may include:***				
1) Checking all vessel stores more extensively;				
2) Restricting or suspending delivery of vessel stores and bunkers; or				
3) Refusing to accept vessel stores onboard.				
104.285 Security Measures for Monitoring				
a) **General**				
1) Owner/Operator to ensure the implementation of security measures by continuously monitoring through a combination of lighting, watch keepers, security guards, deck watches, waterborne patrols, auto intrusion-detection devices, or surveillance equipment of the following:				
i) Vessel;				
ii) Restricted areas onboard the vessel; and				
iii) Area surrounding the vessel.				
2) The following must be considered when establishing the appropriate level & location of lighting:				
i) Vessel personnel should be able to detect activities on & around vessel on both shore side & waterside;				
ii) Coverage should facilitate personnel identification at access points;				
iii) Coverage may be provided through coordination with the port or facility; and				
iv) Lighting effects (such as glare) and its impact on safety, navigation, and other security activities.				
b) MARSEC Level 1 - Owner/Operator to ensure security measures that *may* be done in coordination with facility to:				
1) Monitor the vessel, particularly vessel access points and restricted areas;				
2) Be able to conduct emergency searches of the vessel;				
3) Ensure that equipment or system failures or malfunctions are identified and corrected;				
4) Ensure that automatic intrusion detection device sets off audible/visual alarm at location continuously attended or monitored;				
5) Illuminate deck and access points from sunset to sunrise to enable ID of persons seeking access to vessel; and				
6) Use maximum available lighting underway from sunset to sunrise consistent with safety and international regs.				
c) **MARSEC Level 2** - In addition to security measures at Level 1, additional security measures ***may include:***				
1) Increasing the frequency and details of security patrols;				
2) Increasing the intensity and coverage of lighting, alone or in conjunction with facility;				
3) Using or increasing the use of security/surveillance equipment.				
4) Assigning additional personnel as security lookouts;				
5) Coordinating with boat patrols when provided; or				
6) Coordinating with shoreside foot or vehicle patrols; when provided.				
d) **MARSEC Level 3** - In addition to security measures at Levels 1 and 2, additional security measures ***may include*** the following:				

1) Cooperating with responders and facilities;				
2) Switching on all lights;				
3) Illuminating the vicinity of the vessel;				
4) Activating all surveillance equipment capable of recording activities on or in vicinity of the vessel;				
5) Maximizing the length of time such surveillance equipment can continue to record;				
6) Preparing for underwater inspection of the hull; and				
7) Initiating measures i.e. slow revolution of propeller(s), to deter underwater access to the vessel hull.				
104.290 Security Incident Procedures				
For each MARSEC Level, the Owner/Operator must ensure the VSO & vessel security personnel are able to:				
a) Respond to security threats or breaches of security and maintain critical vessel and vessel-to- facility operations to include:				
1) To prohibit entry into affected area;				
2) Deny access to the vessel except to those responding to the emergency;				
3) Implement MARSEC Level 3 security measures throughout the vessel;				
4) Stopping cargo handling operations; and				
5) Notify shore side authorities or other vessels of the emergency;				
b) Evacuating the vessel in case of security threats or breaches of security;				
c) Reporting security incidents as required in 101.305;				
d) Briefing all vessel personnel on possible threats and the need for vigilance as well as soliciting their assistance; and				
e) Securing non-critical operations in order to focus response on critical operations.				
104.292 Additional Requirements - Passenger Vessels and Ferries				
a) At all MARSEC Levels, the Owner/Operator must ensure that security sweeps are performed prior to getting underway and after any period the vessel was unattended.				
b) As an alternative to ID checks and passenger requirements in 33 CFR 104.265 (f)(2), (f)(4), and (f)(9), the Owner/Operator may ensure security measures are implemented that include:				
1) Searching selected areas prior to embarking passengers and prior to sailing; and				
2) Implementing one or more of the following:				
i) Performing routine security patrols;				
ii) Providing additional closed circuit TV's to monitor passenger areas; or				
iii) Securing all non passenger areas.				
c) Passenger vessels certificated to carry > 2000 passengers working in coordination with the terminal may be subject to additional vehicle screening requirements in accordance with a MARSEC Directive or other orders issued by the Coast Guard.				
d) Owners and operators of passenger vessels covered by this Part that use public access facilities (33 CFR 101.105) must address security measures for the vessel-public access facility interface per the appropriate Area Maritime Security Plan (AMSP).				
e) At MARSEC Level 2 - Owner/Operator must ensure, in addition to Level 1 measures, the implementation of the following:				
1) Search selected areas prior to embarking passengers and prior to sailing;				
2) Passenger vessels certificated to carry < 2000 passengers may be subject to additional vehicle screening requirements in accordance with a MARSEC Directive or other orders issued by the Coast Guard; and				

3) As an alternative to the ID and screening requirements in Part 104.265 (f) (4) and (g)(1) intensify patrols, security sweeps and monitoring identified in paragraph b) of this section.				
f) **At MARSEC Level 3** - Owner/Operator in addition to Levels 1 and 2, as an alternative to the ID checks and passenger screening requirements in Part 104.265 (f)(4) and (h)(1) , ensure that random armed security patrols are conducted, which need not consist of vessel personnel.				
104.295 Additional Requirements - Cruise Ships				
a) **At all MARSEC Levels the Owner/Operator must ensure:**				
1) Screen all persons, baggage and personal effects for dangerous substances and devices;				
2) Check the ID of all persons seeking to board the vessel; this check includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, gov't ID etc;				
3) Perform security patrols; and				
4) Search selected areas prior to embarking passengers and prior to sailing.				
b) **At MARSEC Level 3**, the Owner/Operator must ensure that security briefs are given to passengers about the specific threat.				
PAC 41-04 Shipyard Security				
a) If plan is not in 100% implementation in layup or shipyard status. Shipyard Security requirements must be addressed in the VSP for vessels in layup or shipyard status.				
1) What security measures are maintained onboard the vessel;				
2) How is security re-established before the vessel goes back into service?				
MARSEC Directive 104-6 Guidelines for US Vessels Operating in High Risk Areas				
a) MARSEC Level 2 security measures must be implemented.				
b) Pre-planning/preparation prior to entering high risk waters or ports must be included.				
c) Plans must also address the use of;			✔	Not Required or Submitted Separately
1) Enhanced surveillance and use of lighting;			✔	
2) Surveillance & detection equipment (if applicable);			✔	
3) Crew response if potential attack is detected;			✔	
4) Crew response if attackers gain access to the vessel;			✔	
5) Radio alarm procedures;			✔	
6) Use of SSAS (if applicable);			✔	
c) Reporting procedures after an attack or attempted attack;			✔	
104.415 Amendments and Audits				
a) Amendments				
1) Amendments are approved by the MSC:				
i, ii) May be initiated by owner/operator; if initiated by the Coast Guard, owner operator will have at least 60 days to submit its proposed amendments addressing any matters specified in the notice.				
2) If initiated by owner/operator, proposed amendment must be submitted at least 30 days prior to effective date to the MSC at the address listed in 104.400(b).				
3) Owner/operator shall not be limited to implement additional security measures to address exigent security situations. Owner/operator must notify MSC by most rapid means practicable as to:				
Nature of additional measures				
Circumstances prompting the additional measures				
Period of time expected for these measures				

4) If vessel ownership changes, the VSO must amend the VSP to include the name and contact information of the new vessel owner, and submit affected portion of the VSP for review and approval IAW 104.4				
b) Audits				
1) CSO or VSO must ensure an annual audit of the VSP is conducted beginning no later than one year from initial date of approval and attach certification letter that the VSP meets the applicable requirements.				
2) **VSP must be audited if**:				
Change in company ownership or vessel ownership/operator or				
Modification to vessel, physical structure, emergency response procedures, security measures or operations.				
3) Auditing of VSP as a result vessel modifications may be limited to those sections of the VSP affected by the modifications.				
4) Personnel conducting internal audits of the security measures specified in the VSP or evaluating its implementation must:				
i) have knowledge of methods of conducting audits and inspections, and monitoring techniques;				
ii) not have regularly assigned security duties; and				
iii) be independent of any security measures being audited.				
5) If the audit requires an amendment, the VSO or CSO must submit IAW 104.410, the amendments to the MSC for review and approval NLT 30 days after completion of the audit and a letter certifying the VSP meets the applicable requirements of this part.				
ISPS Part A.5 Declaration of Security (DoS)				
5.4 The DoS shall be completed by:				
5.4.1 The master or the SSO on behalf of the ship(s); and, if appropriate,				
5.4.2 The port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shoreside security, on behalf of the port facility.				
5.5 The DoS shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibilities of each.				
ISPS Part B.9.51 Activities not covered by ISPS Code				
9.51 The SSP should establish details of the procedures and security measures the ship should apply when:				
9.51.1 It is at a port of a State which is not a Contracting Government;				
9.51.2 It is interfacing with a ship to which the Code does not apply;				
9.51.3 It is interfacing with fixed or floating platforms or a mobile drilling unit on location; or				
9.51.4 It is interfacing with a port or port facility which is not required to comply with SOLAS chapter XI-2 and part A of ISPS				

Additional Notes