Title 33 —Navigation and Navigable Waters
Chapter I —Coast Guard, Department of Homeland Security
Subchapter H —Maritime Security

PART 104—MARITIME SECURITY: VESSELS

Authority: 46 U.S.C. 70051, 70116, Chapter 701; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; DHS Delegation No. 00170.1, Revision No. 01.3.

Source: USCG-2003-14749, 68 FR 39302, July 1, 2003, unless otherwise noted.

Subpart A—General

§ 104.100 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

§ 104.105 Applicability.

(a) This part applies to the owner or operator of any:

(1) Mobile Offshore Drilling Unit (MODU), cargo, or passenger vessel subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI-1 or Chapter XI-2;

(2) Foreign cargo vessel greater than 100 gross register tons;

(3) Self-propelled U.S. cargo vessel greater than 100 gross register tons subject to 46 CFR subchapter I, except commercial fishing vessels inspected under 46 CFR part 105;

(4) Vessel subject to 46 CFR chapter I, subchapter L;

(5) Passenger vessel subject to 46 CFR chapter I, subchapter H;

(6) Passenger vessel certificated to carry more than 150 passengers;

(7) Other passenger vessel carrying more than 12 passengers, including at least one passenger-for-hire, that is engaged on an international voyage;

(8) Barge subject to 46 CFR chapter I, subchapters D or O;

(9) Barge carrying certain dangerous cargo in bulk or barge that is subject to 46 CFR Chapter I, subchapter I, that is engaged on an international voyage.

(10) Tankship subject to 46 CFR chapter I, subchapters D or O; and

(11) Towing vessel greater than eight meters in registered length that is engaged in towing a barge or barges subject to this part, except a towing vessel that—

(i) Temporarily assists another vessel engaged in towing a barge or barges subject to this part;

(ii) Shifts a barge or barges subject to this part at a facility or within a fleeting facility;

(iii) Assists sections of a tow through a lock; or

(iv) Provides emergency assistance.

(b) An owner or operator of any vessel not covered in paragraph (a) of this section is subject to parts 101 through 103 of this subchapter.

(c) Foreign Vessels that have on board a valid International Ship Security Certificate that certifies that the verifications required by part A, Section 19.1, of the International Ship and Port Facility Security (ISPS) Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed will be deemed in compliance with this part, except for §§ 104.240, 104.255, 104.292, and 104.295, as appropriate. This includes ensuring that the vessel meets the applicable requirements of SOLAS Chapter XI-2 (Incorporated by reference, see § 101.115 of this subchapter) and the ISPS Code, part A, having taken into account the relevant provisions of the ISPS Code, part B, and that the vessel is provided with an approved security plan.

(d) The TWIC requirements found in parts 101 and 104 of this subchapter do not apply to foreign vessels.

(e) The TWIC requirements found in this part do not apply to mariners employed aboard vessels moored at U.S. facilities only when they are working immediately adjacent to their vessels in the conduct of vessel activities.

(f) Except pursuant to international treaty, convention, or agreement to which the U.S. is a party, this part does not apply to any foreign vessel that is not destined for, or departing from, a port or place subject to the jurisdiction of the U.S. and that is in:

(1) Innocent passage through the territorial sea of the U.S.; or

(2) Transit through the navigable waters of the U.S. that form a part of an international strait.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60513, Oct. 22, 2003; USCG-2004-18057, 69 FR 34925, June 23, 2004; USCG-2004-19963, 70 FR 74669, Dec. 16, 2005; USCG-2006-24196, 72 FR 3579, Jan. 25, 2007; USCG-2007-28915, 81 FR 57710, Aug. 23, 2016]

§ 104.106 Passenger access area.

(a) A ferry, passenger vessel, or cruise ship may designate areas within the vessel as passenger access areas.

(b) A passenger access area is a defined space, within the area over which the owner or operator has implemented security measures for access control, of a ferry, passenger vessel, or cruise ship that is open to passengers. It is not a secure area and does not require a TWIC for unescorted access.

(c) Passenger access areas may not include any areas defined as restricted areas in the VSP.

[USCG-2006-24196, 72 FR 3579, Jan. 25, 2007, as amended by USCG-2008-0179, 73 FR 35009, June 19, 2008]

§ 104.107 Employee access area.

(a) A ferry or passenger vessel, excluding cruise ships, may designate areas within the vessel as employee access areas.

(b) An employee access area is a defined space, within the area over which the owner or operator has implemented security measures for access control, of a ferry or passenger vessel that is open only to employees and not to passengers. It is not a secure area and does not require a TWIC for unescorted access.

(c) Employee access areas may not include any areas defined as restricted areas in the VSP.

[USCG-2006-24196, 72 FR 3579, Jan. 25, 2007]

§ 104.110 Exemptions.

(a) This part does not apply to warships, naval auxiliaries, or other vessels owned or operated by a government and used only on government non-commercial service.

(b) A vessel is not subject to this part while the vessel is laid up, dismantled, or otherwise out of commission.

(c) Vessels with a minimum manning requirement of 20 or fewer TWIC-holding crewmembers are exempt from the requirements in 33 CFR 101.535(a)(1).

[USCG-2003-14749, 68 FR 60513, Oct. 22, 2003, as amended by USCG-2007-28915, 81 FR 57710, Aug. 23, 2016]

§ 104.115 Compliance.

(a) Vessel owners or operators must ensure their vessels are operating in compliance with this part.

(b) Owners or operators of foreign vessels must comply with the following—

(1) Vessels subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI-1 or Chapter XI-2, must carry on board a valid International Ship Security Certificate that certifies that the verifications required by part A, Section 19.1, of the International Ship and Port Facility Security (ISPS) Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed. This includes ensuring that the vessel meets the applicable requirements of SOLAS Chapter XI-2 (Incorporated by reference, see § 101.115 of this chapter) and the ISPS Code, part A, having taken into account the relevant provisions of the ISPS Code, part B, and that the vessel is provided with an approved security plan.

(2) Vessels not subject to SOLAS Chapter XI-1 or Chapter XI-2, may comply with this part through an Alternative Security Program or a bilateral arrangement approved by the Coast Guard. If not complying with an approved Alternative Security Program or bilateral arrangement, these vessels must meet the requirements of paragraph (b) of this section.

(c) By August 23, 2018, owners and operators of vessels subject to this part must amend their Vessel Security Plans to indicate how they will implement the TWIC requirements in this subchapter. By August 23, 2018, owners and operators of vessels subject to this part must operate in accordance with the TWIC provisions found within this subchapter.

[USCG-2003-14749, 68 FR 60513, Oct. 22, 2003, as amended by USCG-2004-18057, 69 FR 34925, June 23, 2004; USCG-2004-19963, 70 FR 74669, Dec. 16, 2005; USCG-2006-25150, 71 FR 39208, July 12, 2006; USCG-2006-24196, 72 FR 3579, Jan. 25, 2007; 73 FR 25565, May 7, 2008; USCG-2007-28915, 81 FR 57710, Aug. 23, 2016]

§ 104.120 Compliance documentation.

(a) Each vessel owner or operator subject to this part must ensure that copies of the following documents are carried on board the vessel and are made available to the Coast Guard upon request:

(1) The approved Vessel Security Plan (VSP) and any approved revisions or amendments thereto, and a letter of approval from the Commanding Officer, Marine Safety Center (MSC);

(2) The VSP submitted for approval and a current acknowledgement letter from the Commanding Officer, MSC, stating that the Coast Guard is currently reviewing the VSP submitted for approval, and that the vessel may continue to operate so long as the vessel remains in compliance with the submitted plan;

(3) For vessels operating under a Coast Guard-approved Alternative Security Program as provided in § 104.140, a copy of the Alternative Security Program the vessel is using, including a vessel specific security assessment report generated under the Alternative Security Program, as specified in § 101.120(b)(3) of this subchapter, and a letter signed by the vessel owner or operator, stating which Alternative Security Program the vessel is using and certifying that the vessel is in full compliance with that program; or

(4) For foreign vessels, subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI-1 or Chapter XI-2, a valid International Ship Security Certificate (ISSC) that attests to the vessel's compliance with SOLAS Chapter XI-2 and the ISPS Code, part A (Incorporated by reference, see § 101.115 of this subchapter) and is issued in accordance with the ISPS Code, part A, section 19. As stated in Section 9.4 of the ISPS Code, part A requires that, in order for the ISSC to be issued, the provisions of part B of the ISPS Code need to be taken into account.

(b) Each owner or operator of an unmanned vessel subject to this part must maintain the documentation described in paragraphs (a)(1), (2), or (3) of this section. The letter required by each of those paragraphs must be carried on board the vessel. The plan or program required by each of those paragraphs must not be carried on board the vessel, but must be maintained in a secure location. During scheduled inspections, the plan or program must be made available to the Coast Guard upon request.

(c) Each vessel owner or operator who designates a passenger or employee access area (as those terms are defined in §§ 104.106 and 104.107 of this part) on their vessel must keep on board the vessel with their approved VSP a clear, visual representation (such as a vessel schematic) of where those designated

areas fall. This need not be submitted to the Coast Guard for approval until incorporated into the VSP at the next VSP submittal (either renewal or amendment), but must be made available to the Coast Guard upon request.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60513, Oct. 22, 2003; USCG-2004-18057, 69 FR 34925, June 23, 2004; USCG-2006-24196, 72 FR 3579, Jan. 25, 2007; USCG-2007-28915, 81 FR 57710, Aug. 23, 2016]

§ 104.125 Noncompliance.

When a vessel must temporarily deviate from the requirements of this part, the vessel owner or operator must notify the cognizant COTP, and either suspend operations or request and receive permission from the COTP to continue operating.

[USCG-2003-14749, 68 FR 60513, Oct. 22, 2003]

§ 104.130 Waivers.

Any vessel owner or operator may apply for a waiver of any requirement of this part that the owner or operator considers unnecessary in light of the nature or operating conditions of the vessel. A request for a waiver must be submitted in writing with justification to the Commandant (CG-5P), Attn: Assistant Commandant for Prevention Policy, U.S. Coast Guard Stop 7501, 2703 Martin Luther King Jr. Avenue SE., Washington, DC 20593-7501. The Commandant (CG-5P) may require the vessel owner or operator to provide additional data for determining the validity of the requested waiver. The Commandant (CG-5P) may grant, in writing, a waiver with or without conditions only if the waiver will not reduce the overall security of the vessel, its passengers, its crew, or its cargo, or facilities or ports that the vessel may visit.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended by USCG-2008-0179, 73 FR 35009, June 19, 2008; USCG-2010-0351, 75 FR 36282, June 25, 2010; USCG-2013-0397, 78 FR 39173, July 1, 2013; USCG-2014-0410, 79 FR 38432, July 7, 2014]

§ 104.135 Equivalents.

For any measure required by this part, the vessel owner or operator may propose an equivalent as provided in § 101.130 of this subchapter.

§ 104.140 Alternative Security Programs.

A vessel owner or operator may use an Alternative Security Program as approved under § 101.120 of this subchapter if:

(a) The Alternative Security Program is appropriate to that class of vessel;

(b) The vessel is not subject to the International Convention for Safety of Life at Sea, 1974; and

(c) The Alternative Security Program is implemented in its entirety.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60513, Oct. 22, 2003]

§ 104.145 Maritime Security (MARSEC) Directive.

Each vessel owner or operator subject to this part must comply with any instructions contained in a MARSEC Directive issued under § 101.405 of this subchapter.

§ 104.150 Right to appeal.

Any person directly affected by a decision or action taken under this part, by or on behalf of the Coast Guard, may appeal as described in § 101.420 of this subchapter.

Subpart B—Vessel Security Requirements

§ 104.200 Owner or operator.

(a) Each vessel owner or operator must ensure that the vessel operates in compliance with the requirements of this part.

(b) For each vessel, the vessel owner or operator must:

(1) Define the security organizational structure for each vessel and provide all personnel exercising security duties or responsibilities within that structure with the support needed to fulfill security obligations;

(2) Designate, in writing, by name or title, a Company Security Officer (CSO), a Vessel Security Officer (VSO) for each vessel, and identify how those officers can be contacted at any time;

(3) Ensure personnel receive training, drills, and exercises enabling them to perform their assigned security duties;

(4) Inform vessel personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;

(5) Ensure vessel security records are kept;

(6) Ensure that adequate coordination of security issues takes place between vessels and facilities; this includes the execution of a Declaration of Security (DoS);

(7) Ensure coordination of shore leave, transit, or crew change-out for vessel personnel, as well as access through the facility of visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with facility operators in advance of a vessel's arrival. Vessel owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations in coordinating such leave;

(8) Ensure security communication is readily available;

(9) Ensure coordination with and implementation of changes in Maritime Security (MARSEC) Level;

(10) Ensure that security systems and equipment are installed and maintained;

(11) Ensure that vessel access, including the embarkation of persons and their effects, is controlled;

(12) Ensure that TWIC procedures are implemented as set forth in this subchapter, including;

(i) Ensuring that only individuals who hold a TWIC and are authorized to be in secure areas are permitted to escort;

(ii) Identifying what action is to be taken by an escort, or other authorized individual, should individuals under escort engage in activities other than those for which escorted access was granted; and

(iii) Notifying vessel employees, and passengers if applicable, of what parts of the vessel are secure areas, employee access areas, and passenger access areas, as applicable, and ensuring such areas are clearly marked.

(13) Ensure that restricted areas are controlled and TWIC provisions are coordinated, if applied to such restricted areas;

(14) Ensure that protocols consistent with § 101.550(a) of this subchapter, for dealing with individuals requiring access who report a lost, damaged, or stolen TWIC, or who have applied for and not yet received a TWIC, are in place;

(15) Ensure that cargo and vessel stores and bunkers are handled in compliance with this part;

(16) Ensure restricted areas, deck areas, and areas surrounding the vessel are monitored;

(17) Provide the Master, or for vessels on domestic routes only, the CSO, with the following information:

(i) Parties responsible for appointing vessel personnel, such as vessel management companies, manning agents, contractors, concessionaires (for example, retail sales outlets, casinos, etc.);

(ii) Parties responsible for deciding the employment of the vessel, including time or bareboat charters or any other entity acting in such capacity; and

(iii) In cases when the vessel is employed under the terms of a charter party, the contract details of those documents, including time or voyage charters; and

(18) Give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods; and

(19) If applicable, ensure that protocols consistent with § 104.267 of this part, for dealing with newly hired employees who have applied for and not yet received a TWIC, are in place.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended by USCG-2003-14749, 68 FR 60513, Oct. 22, 2003; USCG-2006-24196, 72 FR 3579, Jan. 25, 2007; USCG-2013-0397, 78 FR 39173, July 1, 2013; USCG-2007-28915, 81 FR 57710, Aug. 23, 2016]

§ 104.205 Master.

(a) Nothing in this part is intended to permit the Master to be constrained by the Company, the vessel 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 vessel. 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.

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

(1) The Master must, as soon as practicable, inform the nearest COTP. If the vessel is on a foreign voyage, the Master must promptly inform the Coast Guard via the NRC at 1-800-424-8802, direct telephone at 202-267-2675; Fax: 202-267-1322, TDD at 202-267-4477, or E-mail at *HQS-DG-lst-NRCINFO@uscg.mil* and if subject to the jurisdiction of a foreign government, the relevant maritime authority of that foreign government;

(2) The temporary security measures must, to the highest possible degree, be commensurate with the prevailing Maritime Security (MARSEC) Level; and

(3) The owner or operator must ensure that such conflicts are resolved to the satisfaction of the cognizant COTP, or for vessels on international voyages, the Commandant (CG-5P), and that the possibility of recurrence is minimized.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60513, Oct. 22, 2003; USCG-2006-25150, 71 FR 39208, July 12, 2006; USCG-2008-0179, 73 FR 35009, June 19, 2008; USCG-2013-0397, 78 FR 39173, July 1, 2013]

§ 104.210 Company Security Officer (CSO).

(a) ***General.***

(1) Each vessel owner or operator must designate in writing a CSO.

(2) A vessel owner or operator may designate a single CSO for all its vessels to which this part applies, or may designate more than one CSO, in which case the owner or operator must clearly identify the vessels for which each CSO is responsible.

(3) A CSO may perform other duties within the owner or operator's organization, including the duties of a Vessel Security Officer, provided he or she is able to perform the duties and responsibilities required of a CSO.

(4) The CSO may delegate duties required by this part, but remains responsible for the performance of those duties.

(5) The CSO must maintain a TWIC.

(b) ***Qualifications.***

(1) The CSO must have general knowledge, through training or equivalent job experience, in the following:

(i) Security administration and organization of the company's vessel(s);

(ii) Vessel, facility, and port operations relevant to that industry;

(iii) Vessel and facility security measures, including the meaning and the consequential requirements of the different Maritime Security (MARSEC) Levels;

(iv) Emergency preparedness and response and contingency planning;

(v) Security equipment and systems and their operational limitations;

(vi) Methods of conducting audits, inspection and control and monitoring techniques; and

(vii) Techniques for security training and education, including security measures and procedures.

(2) In addition to knowledge and training in paragraph (b)(1) of this section, the CSO must have general knowledge through training or equivalent job experience in the following, as appropriate:

(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.

(xv) Knowledge of TWIC requirements

(c) ***Responsibilities.*** In addition to those responsibilities and duties specified elsewhere in this part, the CSO must, for each vessel for which he or she has been designated:

(1) Keep the vessel apprised of potential threats or other information relevant to its security;

(2) Ensure a Vessel Security Assessment (VSA) 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 vessel security activities are audited;

(6) Arrange for Coast Guard inspections under 46 CFR part 2;

(7) Ensure the timely or prompt correction of problems identified by audits or inspections;

(8) Enhance security awareness and vigilance within the owner's or operator's organization;

(9) Ensure relevant personnel receive adequate security training;

(10) Ensure communication and cooperation between the vessel and the port and facilities with which the vessel interfaces;

(11) Ensure consistency between security requirements and safety requirements;

(12) Ensure that when sister-vessel or fleet security plans are used, the plan for each vessel reflects the vessel-specific information accurately;

(13) Ensure compliance with an Alternative Security Program or equivalents approved under this subchapter, 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.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60513, Oct. 22, 2003; USCG-2006-24196, 72 FR 3580, Jan. 25, 2007]

§ 104.215 Vessel Security Officer (VSO).

(a) ***General.***

(1) A VSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and responsibilities required of the VSO for each such vessel.

(2) For manned vessels, the VSO must be the Master or a member of the crew.

(3) For unmanned vessels, the VSO must be an employee of the company, and the same person may serve as the VSO for more than one unmanned vessel. If a person serves as the VSO for more than one unmanned vessel, the name of each unmanned vessel for which he or she is the VSO must be listed in the Vessel Security Plan (VSP).

(4) The VSO of any unmanned barge and the VSO of any towing vessel interfacing with the barge must coordinate and ensure the implementation of security measures applicable to both vessels during the period of their interface.

(5) The VSO may assign security duties to other vessel personnel; however, the VSO remains responsible for these duties.

(6) The VSO must maintain a TWIC.

(b) ***Qualifications.*** The VSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Those items listed in § 104.210 (b)(1) and (b)(2) of this part;

(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 while at sea; and

(7) TWIC.

(c) ***Certification required.*** After July 1, 2009, persons performing duties as VSO on-board a seagoing vessel subject to the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978, as amended, must hold a valid Coast Guard-issued credential with a Vessel Security

Officer endorsement. The Coast Guard will issue this endorsement only if the person meets the requirements in paragraph (d) of this section. This endorsement serves as proof that the person meets the ship security officer requirements of Regulation VI/5 of the STCW.

(d) ***Requirements for Coast Guard Endorsement:***

(1) To qualify for a VSO endorsement, a person must:

(i) Be at least 18 years of age;

(ii) Be able to speak and understand the English language as would be relevant to the duties of a VSO;

(iii) Hold any valid Coast Guard-issued credential under the regulations specified in 46 CFR Subchapter B;

(iv) Successfully complete a Coast Guard-accepted VSO course;

(v) Sea Service. Fulfill one of the following:

(A) Have approved sea service of not less than 12 months on any vessel subject to § 104.105 of this part, credited in accordance with 46 CFR 10.205(e), 10.211, and/or 10.213; or

(B) Have approved sea service of not less than 6 months on any vessel subject to § 104.105 of this part, credited in accordance with 46 CFR 10.205(b), 10.211, and/or 10.213, and have knowledge of vessel operations.

(2) To qualify as a Coast Guard-accepted course a VSO course under paragraph (d)(1)(iv) of this section must require candidates to demonstrate knowledge, understanding, and proficiency in the following competencies:

(i) Maintaining and supervising the implementation of a vessel security plan;

(ii) Assessing security risk, threat and vulnerability;

(iii) Undertaking regular inspections of the vessel to ensure that appropriate security measures are implemented and maintained;

(iv) Ensuring that security equipment and systems, if any, are properly operated, tested and calibrated;

(v) Encouraging security awareness and vigilance; and

(vi) Ensuring compliance with the TWIC program requirements.

(3) Candidates meeting the knowledge of vessel operations requirement under paragraph (d)(1)(v)(B) of this section must provide evidence through training or equivalent job experience, in the following areas:

(i) Basic vessel layout and construction:

(A) Understanding layout, including decks, rooms and space numbering; and

(B) Understanding of various vessel types; and working knowledge of nautical terms and definitions, especially those used to describe areas and parts of a vessel.

(ii) Shipboard organization: familiarity with the various departments and related functions, the titles used for personnel, the roles and responsibilities of these persons, and the chain of command.

(iii) Shipboard safety:

(A) Understanding of the importance of creating and maintaining safe working and living conditions for passengers and crew alike;

(B) General shipboard safety rules, emergency alarms and signals, and responses to and reporting of accidents;

(C) Proper usage of protective equipment and general knowledge of procedures for entering enclosed spaces;

(D) Proper usage of lifesaving equipment and where such equipment is normally stowed aboard various vessel types;

(E) Understanding of the operating principles of and proper use of watertight and fire screen doors; and

(F) Understanding where it is safe to smoke and not safe to smoke on board and in port.

(iv) Protection of the marine environment:

(A) Understanding of vessel personnel's responsibility to preserve the marine environment; and

(B) Basic working knowledge of pollution prevention regulations and techniques.

(v) Familiarity with key definitions, terminology, and operational practices employed in the maritime industry.

(4)

(i) Persons meeting the criteria in paragraphs (d)(4)(i)(A) and (B) of this section prior to the effective date of this regulation may successfully complete a refresher Coast Guard-accepted VSO course no later than July 1, 2009, to fulfill (d)(1)(iv) of this section. Persons must have:

(A) At least six months of VSO experience during the preceding three years; or

(B) Successfully completed a VSO course that was not approved by the Maritime Administration (MARAD) on behalf of the Coast Guard. Maritime Administration approves VSO courses under section 109 of the Maritime Transportation Security Act of 2002, Public Law 107-295.

(ii) To be eligible to take a refresher Coast Guard-accepted VSO course, a person must present to the course provider documentary evidence that he or she meets the criteria in (d)(4)(i) of this section.

(5) Vessel Security Officer courses meeting the training requirements in paragraphs (d)(2) and (d)(4) of this section are subject to Coast Guard acceptance under 46 CFR 10.309(a)(10)(ii).

(6) Vessel Security Officer courses approved by MARAD on behalf of the Coast Guard under section 109 of the Maritime Transportation Security Act of 2002, Public Law 107-295 will be accepted by the Coast Guard under 46 CFR 10.309 as meeting the requirements of paragraphs (d)(1)(iv) and (d)(2) of this section.

(7) Persons who hold a valid "Vessel Security Officer" endorsement may serve as vessel or company personnel with security duties (33 CFR 104.220), and as all other vessel personnel (33 CFR 104.225), without meeting any additional requirements.

(e) ***Responsibilities.*** In addition to those responsibilities and duties specified elsewhere in this part, the VSO must, for each vessel for which he or she has been designated:

(1) Regularly inspect the vessel to ensure that security measures are maintained;

(2) Ensure maintenance and supervision of the implementation of the VSP, and any amendments to the VSP;

(3) Ensure the coordination and handling of cargo and vessel stores and bunkers in compliance with this part;

(4) Propose modifications to the VSP to the Company Security Officer (CSO);

(5) Ensure that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions;

(6) Ensure security awareness and vigilance on board the vessel;

(7) Ensure adequate security training for vessel personnel;

(8) Ensure the reporting and recording of all security incidents;

(9) Ensure the coordinated implementation of the VSP with the CSO and the relevant Facility Security Officer, when applicable;

(10) Ensure security equipment is properly operated, tested, calibrated and maintained; and

(11) Ensure consistency between security requirements and the proper treatment of vessel personnel affected by those requirements.

(12) Ensure TWIC programs are in place and implemented appropriately.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60513, Oct. 22, 2003; USCG-2006-24196, 72 FR 3580, Jan. 25, 2007; USCG-2008-0028, 73 FR 29070, May 20, 2008; 73 FR 34191, June 17, 2008; USCG-2007-28915, 81 FR 57710, Aug. 23, 2016]

§ 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, 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 Vessel Security Plan (VSP);

(l) Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores; and

(m) The meaning and the consequential requirements of the different Maritime Security (MARSEC) Levels.

(n) Relevant aspects of the TWIC program and how to carry them out.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended by USCG-2006-24196, 72 FR 3580, Jan. 25, 2007]

§ 104.225 Security training for all other vessel personnel.

All other vessel personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge of, through training or equivalent job experience in the following, as appropriate:

(a) Relevant provisions of the Vessel Security Plan (VSP);

(b) The meaning and the consequential requirements of the different Maritime Security (MARSEC) 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.

(f) Relevant aspects of the TWIC program and how to carry them out.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60513, Oct. 22, 2003; USCG-2006-24196, 72 FR 3580, Jan. 25, 2007]

§ 104.230 Drill and exercise requirements.

(a) ***General.***

(1) Drills and exercises must test the proficiency of vessel personnel in assigned security duties at all Maritime Security (MARSEC) Levels and the effective implementation of the Vessel Security Plan (VSP). They must enable the Vessel Security Officer (VSO) to identify any related security deficiencies that need to be addressed.

(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the Vessel Security Plan as the result of an increase in the MARSEC Level, provided the vessel reports attainment to the cognizant COTP.

(b) ***Drills.***

(1) The VSO must ensure that at least one security drill is conducted at least every 3 months, except when a vessel is out of service due to repairs or seasonal suspension of operation provided that in such cases a drill must be conducted within one week of the vessel's reactivation. Security drills may be held in conjunction with non-security drills where appropriate.

(2) Drills must test individual elements of the VSP, including response to security threats and incidents. Drills should take into account the types of operations of the vessel, vessel personnel changes, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.

(3) If the vessel is moored at a facility on the date the facility has planned to conduct any drills, the vessel may, but is not required to, participate in the facility's scheduled drill.

(4) Drills must be conducted within one week from whenever the percentage of vessel personnel with no prior participation in a vessel security drill on that vessel exceeds 25 percent.

(5) Not withstanding paragraph (b)(4) of this section, vessels not subject to SOLAS may conduct drills within 1 week from whenever the percentage of vessel personnel with no prior participation in a vessel security drill on a vessel of similar design and owned or operated by the same company exceeds 25 percent.

(c) ***Exercises.***

(1) Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be:

(i) Full scale or live;

(ii) Tabletop simulation or seminar;

(iii) Combined with other appropriate exercises; or

(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be vessel-specific or part of a cooperative exercise program to exercise applicable facility and vessel security plans or comprehensive port exercises.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

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

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60513, Oct. 22, 2003]

§ 104.235 Vessel recordkeeping requirements.

(a) Unless otherwise specified in this section, the Vessel Security Officer must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized deletion, destruction, or amendment. The following records must be kept:

(1) ***Training.*** For training under § 104.225, 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 Vessel Security Plan (VSP);

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

(4) ***Changes in Maritime Security (MARSEC) 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 vessels 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;

(8) ***Annual audit of the VSP.*** For each annual audit, a letter certified by the Company Security Officer or the VSO stating the date the audit was completed; and

(9) ***Electronic Reader/Physical Access Control System (PACS).*** For each individual granted unescorted access to a secure area, the: FASC-N; date and time that unescorted access was granted; and, if captured, the individual's name. Additionally, documentation to demonstrate that the owner or operator has updated the Canceled Card List with the frequency required in § 101.525 of this subchapter.

(c) Any records required by this part must be protected from unauthorized access or disclosure. TWIC reader records and similar records in a PACS are sensitive security information and must be protected in accordance with 49 CFR part 1520.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60514, Oct. 22, 2003; USCG-2007-28915, 81 FR 57710, Aug. 23, 2016]

§ 104.240 Maritime Security (MARSEC) Level coordination and implementation.

(a) The vessel owner or operator must ensure that, prior to entering a port or visiting an Outer Continental Shelf (OCS) facility, all measures are taken that are specified in the Vessel Security Plan (VSP) for compliance with the MARSEC Level in effect for the port or the OCS facility.

(b) When notified of an increase in the MARSEC Level, the vessel owner or operator must ensure:

(1) If a higher MARSEC Level is set for the port in which the vessel is located or is about to enter, the vessel complies, without undue delay, with all measures specified in the VSP for compliance with that higher MARSEC Level;

(2) The COTP is notified as required by § 101.300(c) when compliance with the higher MARSEC Level has been implemented;

(3) For vessels in port, that compliance with the higher MARSEC Level has taken place within 12 hours of the notification; and

(4) If a higher MARSEC Level is set for the OCS facility with which the vessel is interfacing or is about to visit, the vessel complies, without undue delay, with all measures specified in the VSP for compliance with that higher MARSEC Level.

(c) For MARSEC Levels 2 and 3, the Vessel Security Officer must brief all vessel personnel of identified threats, emphasize reporting procedures, and stress the need for increased vigilance.

(d) An owner or operator whose vessel is not in compliance with the requirements of this section must inform the COTP and obtain approval prior to entering any port, prior to interfacing with another vessel or with a facility or to continuing operations.

(e) For MARSEC Level 3, in addition to the requirements in this part, a vessel owner or operator may be required to implement additional measures, pursuant to 33 CFR part 6, 160 or 165, as appropriate, which may include but are not limited to:

(1) Arrangements to ensure that the vessel can be towed or moved if deemed necessary by the Coast Guard;

(2) Use of waterborne security patrol;

(3) Use of armed security personnel to control access to the vessel and to deter, to the maximum extent practical, a TSI; or

(4) Screening the vessel for the presence of dangerous substances and devices underwater or other threats.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60514, Oct. 22, 2003]

§ 104.245 Communications.

(a) The Vessel Security Officer must have a means to effectively notify vessel personnel of changes in security conditions on board the vessel.

(b) Communications systems and procedures must allow effective and continuous communication between the vessel security personnel, facilities interfacing with the vessel, vessels interfacing with the vessel, and national or local authorities with security responsibilities.

(c) Communication systems and procedures must enable vessel personnel to notify, in a timely manner, shore side authorities or other vessels of a security threat or incident on board.

§ 104.250 Procedures for interfacing with facilities and other vessels.

(a) The vessel owner or operator must ensure that there are measures for interfacing with facilities and other vessels at all MARSEC Levels.

(b) For each U.S. flag vessel that calls on foreign ports or facilities, the vessel owner or operator must ensure procedures for interfacing with those ports and facilities are established.

§ 104.255 Declaration of Security (DoS).

(a) Each vessel owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from a facility or other vessel.

(b) At MARSEC Level 1, the Master or Vessel Security Officer (VSO), or their designated representative, of any cruise ship or manned vessel carrying Certain Dangerous Cargoes, in bulk, must complete and sign a DoS with the VSO or Facility Security Officer (FSO), or their designated representative, of any vessel or facility with which it interfaces.

(1) For a vessel-to-facility interface, prior to arrival of a vessel to a facility, the FSO and Master, VSO, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility. Upon a vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the FSO or Master, VSO, or designated representatives must sign the written DoS.

(2) For a vessel engaging in a vessel-to-vessel activity, prior to the activity, the respective Masters, VSOs, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, VSOs, or designated representatives must sign the written DoS.

(c) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, VSOs, or designated representatives must sign the written DoS.

(d) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period the vessel is at the facility. Upon the vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective FSO and Master, VSO, or designated representatives must sign the written DoS.

(e) At MARSEC Levels 1 and 2, VSOs of vessels that frequently interface with the same facility may implement a continuing DoS for multiple visits, provided that:

(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 the MARSEC Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS must be signed and implemented in accordance with this section.

(g) The COTP may require at any time, at any MARSEC Level, any manned vessel subject to this part to implement a DoS with the VSO or FSO prior to any vessel-to-vessel activity or vessel-to-facility interface when he or she deems it necessary.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60514, Oct. 22, 2003]

§ 104.260 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated and maintained according to the manufacturer's recommendation.

(b) The results of testing completed under paragraph (a) of this section must be recorded in accordance with § 104.235. Any deficiencies must be promptly corrected.

(c) The Vessel Security Plan (VSP) must include procedures for identifying and responding to security system and equipment failures or malfunctions.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended by USCG-2007-28915, 81 FR 57710, Aug. 23, 2016]

§ 104.263 Risk Group classifications for vessels.

(a) For purposes of the Transportation Worker Identification Credential requirements of this subchapter, the following vessels subject to this part are in Risk Group A:

(1) Vessels that carry Certain Dangerous Cargoes in bulk.

(2) Vessels certificated to carry more than 1,000 passengers.

(3) Any vessel engaged in towing a vessel subject to paragraph (a)(1) or (a)(2) of this section.

(b) Vessels may move from one Risk Group classification to another, based on the cargo they are carrying or handling at any given time. An owner or operator expecting a vessel to move between Risk Groups must explain, in the Vessel Security Plan, the timing of such movements, as well as how the vessel will move between the requirements of the higher and lower Risk Groups, with particular attention to the security measures to be taken moving from a lower Risk Group to a higher Risk Group.

[USCG-2007-28915, 81 FR 57711, Aug. 23, 2016]

§ 104.265 Security measures for access control.

(a) ***General.*** The vessel owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on board;

(3) Control access to the vessel; and

(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. Individuals seeking unescorted access to a secure area on a vessel in Risk Group A must pass electronic TWIC inspection and those seeking unescorted access to a secure area on a vessel not in Risk Group A must pass either electronic TWIC inspection or visual TWIC inspection.

(b) The vessel owner or operator must ensure that 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 identification of the types of restriction or prohibition to be applied and the means of enforcing them;

(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 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.

(d) ***MARSEC Level 1.*** The vessel owner or operator must ensure security measures in this paragraph are implemented to:

(1) Implement a TWIC Program as set out in subpart E of part 101 of this subchapter, as applicable, and in accordance with the vessel's assigned Risk Group, as set out in § 104.263;

(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 inspection; and

(ii) Failure to consent or submit to screening or 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 surveyor 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) Deter unauthorized access to the vessel;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Lock or otherwise prevent access to unattended spaces that adjoin areas to which passengers and 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 on board, including repelling unauthorized boarders.

(e) ***MARSEC Level 2.*** In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(1) Increasing the frequency and detail of screening of people, personal effects, and vehicles being embarked or loaded onto the vessel as specified for MARSEC Level 2 in the approved VSP, except for government-owned vehicles on official business when government personnel present identification credentials for entry;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to patrol deck areas during periods of reduced vessel operations to deter unauthorized access;

(4) Limiting the number of access points to the vessel by closing and securing some access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the vessel, which may include, in liaison with the facility, providing boat patrols;

(7) Establishing a restricted area on the shore side of the vessel, in close cooperation with the facility; or

(8) Implementing additional electronic TWIC inspection requirements, as required by § 104.263, and by subpart E of part 101 of this subchapter, if relevant.

(f) ***MARSEC Level 3.*** In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. The additional security measures may include:

(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 extensively, for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage on board;

(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 thereof;

(6) Suspending embarkation and/or disembarkation of personnel;

(7) Suspending cargo operations;

(8) Evacuating the vessel;

(9) Moving the vessel;

(10) Preparing for a full or partial search of the vessel; or

(11) Implementing additional electronic TWIC inspection requirements, as required by § 104.263, and by subchapter E of part 101 of this subchapter, if relevant.

[USCG-2006-24196, 72 FR 3580, Jan. 25, 2007, as amended by USCG-2007-28915, 81 FR 57711, Aug. 23, 2016]

§ 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.

(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 (*https://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.

[USCG-2006-24196, 72 FR 3581, Jan. 25, 2007, as amended by USCG-2013-0397, 78 FR 39173, July 1, 2013; USCG-2007-28915, 81 FR 57711, Aug. 23, 2016; USCG-2022-0323, 88 FR 10029, Feb. 16, 2023]

§ 104.270 Security measures for restricted areas.

(a) ***General.*** The vessel owner or operator must ensure the designation of restricted areas in order to:

(1) Prevent or deter unauthorized access;

(2) Protect persons authorized to be on board;

(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.*** The vessel owner or operator must ensure restricted areas are designated on board the vessel, as specified in the approved plan. Restricted areas must include, as appropriate:

(1) Navigation bridge, machinery spaces and other control stations;

(2) Spaces containing security and surveillance equipment and systems and their controls and lighting system controls;

(3) Ventilation and air-conditioning 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 vessel stores;

(8) Crew accommodations; and

(9) Any other spaces or areas vital to the security of the vessel.

(c) The vessel owner or operator must ensure that security 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 indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

(d) ***Maritime Security (MARSEC) Level 1.*** The vessel owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

(1) Locking or securing access points;

(2) Monitoring and using surveillance equipment;

(3) Using guards or patrols; and

(4) Using automatic intrusion detection devices, which if used must activate an audible and/or visual alarm at a location that is continuously attended or monitored, to alert vessel personnel to unauthorized access.

(e) ***MARSEC Level 2.*** In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(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 the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may include:

(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.*** The vessel owner or operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the facility or another vessel, are specified in order to:

(1) Deter tampering;

(2) Prevent cargo that is not meant for carriage from being accepted and stored on board 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 or repeated cargo operations with the same shipper, coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

(b) ***Maritime Security (MARSEC) Level 1.*** At MARSEC Level 1, the vessel owner or 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 that cargo markings or container numbers match the information provided with shipping documents;

(3) Ensure, in liaison with the facility, that vehicles to be loaded on board car carriers, RO-RO, and passenger ships are subjected to screening prior to loading, in accordance with the frequency required in the VSP; and

(4) Check, in liaison with the facility, seals or other methods used to prevent tampering.

(c) ***MARSEC Level 2.*** In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved Vessel Security Plan (VSP). These additional security measures may include:

(1) Increasing the frequency and detail of checking cargo and cargo spaces for evidence of tampering;

(2) Intensifying checks to ensure that only the intended cargo, container, or other cargo transport units are loaded;

(3) Intensifying screening of vehicles to be loaded on car-carriers, RO-RO, and passenger vessels;

(4) In liaison with the facility, increasing frequency and detail in checking seals or other methods used to prevent tampering;

(5) Increasing the frequency and intensity of visual and physical inspections; or

(6) Coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

(d) ***MARSEC Level 3.*** In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures 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.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60514, Oct. 22, 2003]

§ 104.280 Security measures for delivery of vessel stores and bunkers.

(a) ***General.*** The vessel owner or operator must ensure that security measures relating to the delivery of vessel stores and 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. For vessels that routinely use a facility, a vessel owner or operator may establish and implement standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation.

(b) ***Maritime Security (MARSEC) Level 1.*** At MARSEC Level 1, the vessel owner or operator must ensure the implementation of measures to:

(1) Check vessel stores before being accepted;

(2) Check that vessel stores and bunkers match the order prior to being brought on board or being bunkered; and

(3) Ensure that vessel stores are controlled or immediately and securely stowed following delivery.

(c) ***MARSEC Level 2.*** In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved Vessel Security Plan (VSP). These additional security measures may include:

(1) Intensifying inspection of the vessel stores during delivery; or

(2) Checking vessel stores prior to receiving them on board.

(d) ***MARSEC Level 3.*** In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These 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 on board.

§ 104.285 Security measures for monitoring.

(a) ***General.***

(1) The vessel owner or operator must ensure the implementation of security measures and have the capability to continuously monitor, through a combination of lighting, watchkeepers, security guards, deck watches, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment, as specified in their approved Vessel Security Plan (VSP), the—

(i) Vessel;

(ii) Restricted areas on board the vessel; and

(iii) Area surrounding the vessel.

(2) The following must be considered when establishing the appropriate level and location of lighting:

(i) Vessel personnel should be able to detect activities on and around the vessel, on both the shore side and the 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) ***Maritime Security (MARSEC) Level 1.*** At MARSEC Level 1, the vessel owner or operator must ensure the implementation of security measures, which may be done in coordination with a 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 any automatic intrusion detection device sets off an audible or visual alarm, or both, at a location that is continuously attended or monitored;

(5) Light deck and vessel 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 vessel; and

(6) Use maximum available lighting while underway, during the period between sunset and sunrise, consistent with safety and international regulations.

(c) ***MARSEC Level 2.*** In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(1) Increasing the frequency and detail of security patrols;

(2) Increasing the coverage and intensity of lighting, alone or in coordination with the facility;

(3) Using or increasing the use of security and surveillance equipment;

(4) Assigning additional personnel as security lookouts;

(5) Coordinating with boat patrols, when provided; and

(6) Coordinating with shoreside foot or vehicle patrols, when provided.

(d) ***MARSEC Level 3.*** In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may include:

(1) Cooperating with responders and facilities;

(2) Switching on all lights;

(3) Illuminating the vicinity of the vessel;

(4) Switching on all surveillance equipment capable of recording activities on, or in the 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, including the slow revolution of the vessel's propellers, if practicable, to deter underwater access to the hull of the vessel.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60514, Oct. 22, 2003]

§ 104.290 Security incident procedures.

For each Maritime Security (MARSEC) Level, the vessel owner or operator must ensure the Vessel Security Officer (VSO) and vessel security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical vessel and vessel-to-facility interface operations, to include:

(1) Prohibiting entry into affected area;

(2) Denying access to the vessel, except to those responding to the emergency;

(3) Implementing MARSEC Level 3 security measures throughout the vessel;

(4) Stopping cargo-handling operations; and

(5) Notifying shoreside 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, soliciting their assistance in reporting suspicious persons, objects, or activities; 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 Maritime Security (MARSEC) Levels, the vessel owner or operator must ensure security sweeps are performed, prior to getting underway, after any period the vessel was unattended.

(b) As an alternative to the identification checks and passenger screening requirements in § 104.265(d)(2), (d)(4), and (d)(9), the owner or operator of a passenger vessel or ferry 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 television to monitor passenger areas; or

(iii) Securing all non-passenger areas.

(c) Passenger vessels 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 MARSEC Directive or other orders issued by the Coast Guard.

(d) Owners and operators of passenger vessels and ferries covered by this part that use public access facilities, as that term is defined in § 101.105 of this subchapter, must address security measures for the interface of the vessel and the public access facility, in accordance with the appropriate Area Maritime Security Plan.

(e) At MARSEC Level 2, a vessel owner or operator must ensure, in addition to MARSEC 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 less than 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; and

(3) As an alternative to the identification and screening requirements in § 104.265(d)(4) and (e)(1), intensify patrols, security sweeps and monitoring identified in paragraph (b) of this section.

(f) At MARSEC Level 3, a vessel owner or operator may, in addition to MARSEC Levels 1 and 2 measures, as an alternative to the identification checks and passenger screening requirements in § 104.265(d)(4) and (f)(1), ensure that random armed security patrols are conducted, which need not consist of vessel personnel.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60514, Oct. 22, 2003; USCG-2008-0179, 73 FR 35009, June 19, 2008; USCG-2007-28915, 81 FR 57711, Aug. 23, 2016]

§ 104.295 Additional requirements—cruise ships.

(a) At all MARSEC Levels, the owner or operator of a cruise ship must ensure the following:

(1) Screen all persons, baggage, and personal effects for dangerous substances and devices prior to entering the sterile or secure portion of a cruise ship in accordance with the qualification, training, and equipment requirements of §§ 105.530, 105.535, and 105.545 of this subchapter.

(2) The vessel owner or operator may work with the owner or operator of each cruise ship terminal or port of call at which that vessel embarks or disembarks passengers to meet the requirements of this section. The owner or operator of a cruise ship need not duplicate any provisions fulfilled by the cruise ship terminal or port of call. When a provision is fulfilled by the cruise ship terminal or port of call, the applicable section of the Vessel Security Plan must refer to that fact.

(3) Perform security patrols; and

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

(b) At MARSEC Level 3, the owner or operator of a cruise ship must ensure that security briefs to passengers about the specific threat are provided.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended by USCG-2006-23846, 83 FR 12102, Mar. 19, 2018]

§ 104.297 Additional requirements—vessels on international voyages.

(a) An owner or operator of a U.S. flag vessel, 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-2 and the ISPS Code, part A (Incorporated by reference, see § 101.115 of this subchapter).

(b) Owners or operators of U.S. flag vessels 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 vessel. This certificate must be issued by the Coast Guard.

(c) Owners or operators of vessels 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 Sector Office of the port where the vessel 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 on or before July 1, 2004.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60515, Oct. 22, 2003; USCG-2006-25556, 72 FR 36328, July 2, 2007]

Subpart C—Vessel Security Assessment (VSA)

§ 104.300 General.

(a) The Vessel Security Assessment (VSA) is a written document that is based on the collection of background information and the completion and analysis of an on-scene survey.

(b) A single VSA may be performed and applied to more than one vessel to the extent that they share physical characteristics and operations.

(c) Third parties may be used in any aspect of the VSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a VSA should be able to draw upon expert assistance in the following areas:

(1) Knowledge of current security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Techniques used to circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on vessel structures and equipment;

(7) Vessel security requirements;

(8) Vessel-to-vessel activity and vessel-to-facility interface business practices;

(9) Contingency planning, emergency preparedness and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine engineering; and

(13) Vessel and port operations.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60515, Oct. 22, 2003]

§ 104.305 Vessel Security Assessment (VSA) requirements.

(a) ***Background.*** The vessel owner or operator must ensure that the following background information is provided to the person or persons who will conduct the on-scene survey and assessment:

(1) General layout of the vessel, including the location of:

(i) Each actual or potential point of access to the vessel and its function;

(ii) Spaces that should have restricted access;

(iii) Essential maintenance equipment;

(iv) Cargo spaces and storage;

(v) Storage of unaccompanied baggage; and

(vi) Vessel stores;

(2) Threat assessments, including the purpose and methodology of the assessment, for the area or areas in which the vessel operates or at which passengers embark or disembark;

(3) The previous VSA, if any;

(4) Emergency and stand-by equipment available to maintain essential services;

(5) Number of vessel personnel and any existing security duties to which they are assigned;

(6) Existing personnel training requirement practices of the vessel;

(7) Existing security and safety equipment for the protection of personnel, visitors, passengers, and vessels personnel;

(8) Escape and evacuation routes and assembly stations that have to be maintained to ensure the orderly and safe emergency evacuation of the vessel;

(9) Existing agreements with private security companies providing waterside or vessel security services; and

(10) Existing security measures and procedures, including:

(i) Inspection and control procedures;

(ii) Identification systems;

(iii) Surveillance and monitoring equipment;

(iv) Personnel identification documents;

(v) Communication systems;

(vi) Alarms;

(vii) Lighting;

(viii) Access control systems; and

(ix) Other security systems.

(b) ***On-scene survey.*** The vessel owner or operator must ensure that an on-scene survey of each vessel is conducted. The on-scene survey is to verify or collect information required in paragraph (a) of this section. It consists of an actual survey that examines and evaluates existing vessel protective measures, procedures, and operations for:

(1) Ensuring performance of all security duties;

(2) Controlling access to the vessel, through the use of identification systems or otherwise;

(3) Controlling the embarkation of vessel personnel and other persons and their effects, including personal effects and baggage whether accompanied or unaccompanied;

(4) Supervising the handling of cargo and the delivery of vessel stores;

(5) Monitoring restricted areas to ensure that only authorized persons have access;

(6) Monitoring deck areas and areas surrounding the vessel; and

(7) The ready availability of security communications, information, and equipment.

(c) ***Analysis and recommendations.*** In conducting the VSA, the Company Security Officer (CSO) must analyze the vessel background information and the on-scene survey, and while considering the requirements of this part, provide recommendations for the security measures the vessel should include in the Vessel Security Plan (VSP). This includes but is not limited to the following:

(1) Restricted areas;

(2) Response procedures for fire or other emergency conditions;

(3) Security supervision of vessel personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;

(4) Frequency and effectiveness of security patrols;

(5) Access control systems, including identification systems;

(6) Security communication systems and procedures;

(7) Security doors, barriers, and lighting;

(8) Any security and surveillance equipment and systems;

(9) Possible security threats, including but not limited to:

(i) Damage to or destruction of the vessel or an interfacing facility or vessel by dangerous substances and devices, arson, sabotage, or vandalism;

(ii) Hijacking or seizure of the vessel or of persons on board;

(iii) Tampering with cargo, essential vessel equipment or systems, or vessel stores;

(iv) Unauthorized access or use, including presence of stowaways;

(v) Smuggling dangerous substances and devices;

(vi) Use of the vessel to carry those intending to cause a security incident and/or their equipment;

(vii) Use of the vessel itself as a weapon or as a means to cause damage or destruction;

(viii) Attacks from seaward while at berth or at anchor; and

(ix) Attacks while at sea; and

(10) Evaluating the potential of each identified point of access, including open weather decks, for use by individuals who might seek to breach security, whether or not those individuals legitimately have access to the vessel.

(d) ***VSA report.***

(1) The vessel owner or 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 possible 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 on board 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) Other areas that may, if damaged or used illicitly, pose a risk to people, property, or operations on board 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.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60515, Oct. 22, 2003]

§ 104.310 Submission requirements.

(a) A completed Vessel Security Assessment (VSA) report must be submitted with the Vessel Security Plan (VSP) required in § 104.410 of this part.

(b) A vessel owner or operator may generate and submit a report that contains the VSA for more than one vessel subject to this part, to the extent that they share similarities in physical characteristics and operations.

(c) The VSA must be reviewed and revalidated, and the VSA report must be updated, each time the VSP is submitted for reapproval or revisions.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60515, Oct. 22, 2003]

Subpart D—Vessel Security Plan (VSP)

§ 104.400 General.

(a) The Company Security Officer (CSO) must ensure a Vessel Security Plan (VSP) is developed and implemented for each vessel. The VSP:

(1) Must identify the CSO and VSO by name or position and provide 24-hour contact information;

(2) Must be written in English, although a translation of the VSP in the working language of vessel personnel may also be developed;

(3) Must address each vulnerability identified in the Vessel Security Assessment (VSA);

(4) Must describe security measures for each MARSEC Level;

(5) Must state the Master's authority as described in § 104.205; and

(6) May cover more than one vessel to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the Commanding Officer, Marine Safety Center.

(b) The VSP must be submitted to the Commanding Officer, Marine Safety Center, U.S. Coast Guard. Send all mail to: Commanding Officer (MSC), Attn: Marine Safety Center, U.S. Coast Guard Stop 7430, 2703 Martin Luther King Jr. Avenue SE., Washington, DC 20593-7430, in a written or electronic format. Information for submitting the VSP electronically can be found at *http://www.uscg.mil/HQ/MSC*. Owners or operators of foreign flag vessels that are subject to SOLAS Chapter XI-1 or Chapter XI-2 must comply with this part by carrying on board a valid International Ship Security Certificate that certifies that the verifications required by Section 19.1 of part A of the ISPS Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed. As stated in Section 9.4 of the ISPS Code, part A requires that, in order for the ISSC to be issued, the provisions of part B of the ISPS Code need to be taken into account.

(c) The VSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the VSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60515, Oct. 22, 2003; USCG-2004-18057, 69 FR 34925, June 23, 2004; USCG-2007-26953, 72 FR 5931, Feb. 8, 2007; USCG-2010-0351, 75 FR 36282, June 25, 2010; USCG-2014-0410, 79 FR 38432, July 7, 2014; USCG-2016-0498, 82 FR 35080, July 28, 2017; USCG-2023-0759, 89 FR 22947, Apr. 3, 2024]

§ 104.405 Format of the Vessel Security Plan (VSP).

(a) A vessel owner or operator must ensure that the VSP consists of the individual sections listed in this paragraph (a). If the VSP does not follow the order as it appears in the list, the vessel owner or operator must ensure that the VSP contains an index identifying the location of each of the following sections:

(1) Security organization of the vessel;

(2) Personnel training;

(3) Drills and exercises;

(4) Records and documentation;

(5) Response to change in MARSEC Level;

(6) Procedures for interfacing with facilities and other vessels;

(7) Declarations of Security (DoS);

(8) Communications;

(9) Security systems and equipment maintenance;

(10) Security measures for access control, including the vessel's TWIC Program, designated passenger access areas and employee access areas;

(11) Security measures for restricted areas;

(12) Security measures for handling cargo;

(13) Security measures for delivery of vessel stores and bunkers;

(14) Security measures for monitoring;

(15) Security incident procedures;

(16) Audits and Vessel Security Plan (VSP) amendments; and

(17) Vessel Security Assessment (VSA) Report.

(b) The VSP must describe in detail how the requirements of subpart B of this part will be met.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended by USCG-2006-24196, 72 FR 3582, Jan. 25, 2007; USCG-2007-28915, 81 FR 57711, Aug. 23, 2016]

§ 104.410 Submission and approval.

(a) In accordance with § 104.115, each vessel owner or operator must either—

(1) Submit one copy of their Vessel Security Plan (VSP), in English, for review and approval to the Commanding Officer, Marine Safety Center (MSC) and a letter certifying that the VSP meets applicable requirements of this part; or

(2) If intending to operate under an Approved Alternative Security Program, a letter signed by the vessel owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) Owners or operators of vessels not in service on or before December 31, 2003, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations.

(c) The Commanding Officer, Marine Safety Center (MSC), will examine each submission for compliance with this part, and either—

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

(d) A VSP may be submitted and approved to cover more than one vessel where the vessel design and operations are similar.

(e) Each company or vessel, owner or operator, that submits one VSP to cover two or more vessels of similar design and operation must address vessel-specific information that includes the physical and operational characteristics of each vessel.

(f) A plan that is approved by the MSC is valid for 5 years from the date of its approval.

[USCG-2003-14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60515, Oct. 22, 2003; USCG-2004-19963, 70 FR 74669, Dec. 16, 2005; USCG-2013-0397, 78 FR 39173, July 1, 2013; USCG-2007-28915, 81 FR 57711, Aug. 23, 2016]

§ 104.415 Amendment and audit.

(a) ***Amendments.***

(1) Amendments to a Vessel Security Plan that are approved by the Marine Safety Center (MSC) may be initiated by:

(i) The vessel owner or operator; or

(ii) The Coast Guard upon a determination that an amendment is needed to maintain the vessel's security. The Coast Guard will give the vessel owner or operator written notice and request that the vessel owner or operator propose amendments addressing any matters specified in the notice. The company owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the company owner or operator shall ensure temporary security measures are implemented to the satisfaction of the Coast Guard.

(2) Proposed amendments must be sent to the MSC at the address shown in § 104.400(b) of this part. If initiated by the company or vessel, owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the MSC allows a shorter period. The MSC will approve or disapprove the proposed amendment in accordance with § 104.410 of this part.

(3) Nothing in this section should be construed as limiting the vessel owner or operator from the timely implementation of such additional security measures not enumerated in the approved VSP as necessary to address exigent security situations. In such cases, the owner or operator must notify

the MSC by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

(4) If the owner or operator has changed, the Vessel Security Officer (VSO) must amend the Vessel Security Plan (VSP) to include the name and contact information of the new vessel owner or operator and submit the affected portion of the VSP for review and approval in accordance with § 104.410 of this part.

(b) ***Audits.***

(1) The CSO or VSO must ensure an audit of the VSP is performed annually, beginning no later than one year from the initial date of approval and attach a letter to the VSP certifying that the VSP meets the applicable requirements of this part.

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

(3) Auditing the VSP as a result of modifications to the vessel may be limited to those sections of the VSP affected by the vessel modifications.

(4) Unless impracticable due to the size and nature of the company or the vessel, 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 control and monitoring techniques;

(ii) Not have regularly assigned security duties; and

(iii) Be independent of any security measures being audited.

(5) If the results of an audit require amendment of either the VSA or VSP, the VSO or CSO must submit, in accordance with § 104.410 of this part, 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 VSP meets the applicable requirements of this part.

[USCG-2003-14749, 68 FR 39302, July 1, 2003; 68 FR 41915, July 16, 2003, as amended at 68 FR 60515, Oct. 22, 2003]