

§ 104.310

33 CFR Ch. I (7-1-08 Edition)

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 re-validated, 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 (MSC), USCG Marine Safety Center, 1900 Half Street, SW., Suite 1000, Room 525, Washington, DC 20024 for visitors. Send all mail to Commanding Officer (MSC), United States Coast Guard, JR10-0525, 2100 2nd Street, SW., Washington, DC 20593, 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]

§ 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 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. VSPs that have been approved by the Coast Guard prior to March 26, 2007, do not need to be