

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]