

Coast Guard, DHS

§ 105.400

(v) Radio and telecommunication systems, including computer systems and networks;

(vi) Relevant transportation infrastructure; and

(vii) Utilities.

(3) The FSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) Facility personnel;

(ii) Passengers, visitors, vendors, repair technicians, vessel personnel, etc.;

(iii) Capacity to maintain emergency response;

(iv) Cargo, particularly dangerous goods and hazardous substances;

(v) Delivery of vessel stores;

(vi) Any facility security communication and surveillance systems; and

(vii) Any other facility security systems, if any.

(4) The FSA report must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on facility personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The FSA report must discuss and evaluate key facility measures and operations, including:

(i) Ensuring performance of all security duties;

(ii) Controlling access to the facility, 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) Procedures for the handling of cargo and the delivery of vessel stores;

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

(vi) Monitoring the facility and areas adjacent to the pier; and

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

(e) The FSA, FSA report, and FSP must be protected from unauthorized access or disclosure.

[USCG-2003-14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003]

§ 105.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan required in § 105.410 of this part.

(b) A facility owner or operator may generate and submit a report that contains the Facility Security Assessment for more than one facility subject to this part, to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP.

(c) The FSA must be reviewed and validated, and the FSA report must be updated each time the FSP is submitted for reapproval or revisions.

[USCG-2003-14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003]

Subpart D—Facility Security Plan (FSP)

§ 105.400 General.

(a) The Facility Security Officer (FSO) must ensure a Facility Security Plan (FSP) is developed and implemented for each facility for which he or she is designated as FSO. The FSP:

(1) Must identify the FSO by name and position, and provide 24-hour contact information;

(2) Must be written in English;

(3) Must address each vulnerability identified in the Facility Security Assessment (FSA);

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

(5) May cover more than one facility to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP.

(b) The FSP must be submitted for approval to the cognizant COTP in a written or electronic format. Information for submitting the FSP electronically can be found at <http://www.uscg.mil/HQ/MS>.

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

§ 105.405

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

[USCG-2003-14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003]

§ 105.405 Format and content of the Facility Security Plan (FSP).

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

- (1) Security administration and organization of the facility;
- (2) Personnel training;
- (3) Drills and exercises;
- (4) Records and documentation;
- (5) Response to change in MARSEC Level;
- (6) Procedures for interfacing with vessels;
- (7) Declaration of Security (DoS);
- (8) Communications;
- (9) Security systems and equipment maintenance;
- (10) Security measures for access control, including designated public 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 security plan amendments;
- (17) Facility Security Assessment (FSA) report; and
- (18) Facility Vulnerability and Security Measures Summary (Form CG-6025) in appendix A to part 105-Facility Vulnerability and Security Measures Summary (CG-6025).

(b) The FSP must describe in detail how the requirements of subpart B of this part will be met. FSPs that have been approved by the Coast Guard prior to March 26, 2007, do not need to be amended to describe their TWIC proce-

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

dures until the next regularly scheduled resubmission of the FSP.

(c) The Facility Vulnerability and Security Measures Summary (Form CG-6025) must be completed using information in the FSA concerning identified vulnerabilities and information in the FSP concerning security measures in mitigation of these vulnerabilities.

[USCG-2003-14732, 68 FR 39322, July 1, 2003, as amended by USCG-2006-24196, 72 FR 3585, Jan. 25, 2007]

§ 105.410 Submission and approval.

(a) On or before December 31, 2003, the owner or operator of each facility currently in operation must either:

(1) Submit one copy of their Facility Security Plan (FSP) for review and approval to the cognizant COTP and a letter certifying that the FSP meets applicable requirements of this part; or

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

(b) Owners or operators of facilities 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 or by December 31, 2003, whichever is later.

(c) The cognizant COTP 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) An FSP may be submitted and approved to cover more than one facility where they share similarities in design and operations, if authorized and approved by each cognizant COTP.

(e) Each facility owner or operator that submits one FSP to cover two or more facilities of similar design and operation must address facility-specific information that includes the design