

§ 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

and operational characteristics of each facility and must complete a separate Facility Vulnerability and Security Measures Summary (Form CG-6025), in appendix A to part 105—Facility Vulnerability and Security Measures Summary (CG-6025), for each facility covered by the plan.

(f) A FSP that is approved by the cognizant COTP is valid for five years from the date of its approval.

[USCG-2003-14732, 68 FR 39322, July 1, 2003; 68 FR 41916, July 16, 2003, as amended at 68 FR 60542, Oct. 22, 2003; USCG-2004-19963, 70 FR 74669, Dec. 16, 2005]

§ 105.415 Amendment and audit.

(a) *Amendments.* (1) Amendments to a Facility Security Plan (FSP) that is approved by the cognizant COTP may be initiated by:

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

(2) Proposed amendments must be submitted to the cognizant COTP. If initiated by the facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant COTP allows a shorter period. The cognizant COTP will approve or disapprove the proposed amendment in accordance with § 105.410 of this subpart.

(3) Nothing in this section should be construed as limiting the facility owner or operator from the timely implementation of such additional security measures not enumerated in the approved FSP as necessary to address exigent security situations. In such cases, the owner or operator must notify the cognizant COTP by the most rapid means practicable as to the na-

ture 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 there is a change in the owner or operator, the Facility Security Officer (FSO) must amend the FSP to include the name and contact information of the new facility owner or operator and submit the affected portion of the FSP for review and approval in accordance with § 105.410 if this subpart.

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

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

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

(4) Unless impracticable due to the size and nature of the company or the facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must:

- (i) Have knowledge of methods for conducting audits and inspections, and security, 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 FSA or FSP, the FSO must submit, in accordance with § 105.410 of this subpart, the amendments to the cognizant COTP for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets the applicable requirements of this part.

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