

(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. Format for submitting the FSP electronically can be found at <http://www.uscg.mil/HQ/MSG>.

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

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

§ 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 facility owner or operator must ensure that the FSP describes in detail how each of the individual requirements of subpart B of this part will be met.

(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.

§ 105.410 Submission and approval.

(a) On or before December 29, 2003, each facility owner or operator must either:

(1) Submit one copy of their Facility Security Plan (FSP) for review and approval to the cognizant COTP; or

(2) If implementing a Coast Guard approved Alternative Security Program, meet the requirements in § 101.120(b) of this subchapter.

(b) Facilities constructed on or after July 1, 2004, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations.

(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, or

(2) 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 the 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.

§ 105.415 Amendment and audit.

(a) *Amendments.* (1) Amendments to a 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 § 105.415 of this subpart.

(3) If there is a change in the owner or operator, the Facility Security Officer (FSO) must amend the Facility Security Plan (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 § 105.415 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