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/MSC*.

(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.

[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 procedures 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]