and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;

(iii) A description of each vulnerability found during the on-scene survey;

(iv) A description of security measures that could be used to address each vulnerability;

(v) A list of the key facility operations that are important to protect; and

(vi) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the facility.

(2) A FSA report must describe the following elements within the facility:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(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.

(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; USCG–2013–0397, 78 FR 39173, July 1, 2013; USCG–2022–0323, 88 FR 10029, Feb. 16, 2023]

§ 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 the facility's TWIC Program and 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;

(18) Facility Vulnerability and Security Measures Summary (Form CG–6025) available at *https://www.dcms.uscg.mil/forms/*;

(19)–(20) [Reserved]

(21) If applicable, cruise ship TSP in accordance with subpart E of this part; and

(22) System for seafarers' access.

(b) The FSP must describe in detail how the 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.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended by USCG–2006–24196, 72 FR 3585, Jan. 25, 2007; USCG–2006–23846, 83 FR 12102, Mar. 19, 2018; USCG–2007–28915, 81 FR 57713, Aug. 23, 2016; USCG-2013-1087, 84 FR 12119, Apr. 1, 2019; USCG–2020–0304, 85 FR 58278, Sept. 18, 2020]

§ 105.410 Submission and approval.

(a) 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 Alternative 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.

(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), for each facility covered by the plan. The form is available at *https://www.dcms.uscg.mil/forms/*.

(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; USCG–2013–0397, 78 FR 39173, July 1, 2013; USCG–2007–28915, 81 FR 57713, Aug. 23, 2016; USCG–2020–0304, 85 FR 58278, Sept. 18, 2020]

§ 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 nature 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]

Subpart E—Facility Security: Cruise Ship Terminals

SOURCE: USCG–2006–23846, 83 FR 12102, Mar. 19, 2018, unless otherwise noted.

§ 105.500 General.

(a) *Applicability*. The owner or operator of a cruise ship terminal must comply with this subpart when receiving a cruise ship or tenders from cruise ships.

(b) *Purpose*. This subpart establishes cruise ship terminal screening programs within the Facility Security Plans to ensure that prohibited items are not present within the secure areas that have been designated for screened persons, baggage, and personal effects, and are not brought onto cruise ships interfacing with the terminal.

(c) *Compliance dates*. (1) No later than October 15, 2018, cruise ship terminal owners or operators must submit, for each terminal, a terminal screening program (TSP) that conforms with the requirements in §105.505 to the cognizant COTP for review and approval.

(2) No later than April 18, 2019, each cruise ship terminal owner or operator must operate in compliance with an approved TSP and this subpart.

§ 105.505 Terminal Screening Program (TSP).

(a) *General requirements*. The owner or operator of a cruise ship terminal must ensure a TSP is developed, added to the Facility Security Plan (FSP), and implemented. The TSP must—

(1) Document all procedures that are employed to ensure all persons, baggage, and personal effects are screened at the cruise ship terminal prior to being allowed into a cruise ship terminal's secure areas or onto a cruise ship;

(2) Be written in English; and

(3) Be approved by the Coast Guard as part of the FSP in accordance with subpart D of this part.

(b) *Availability*. Each cruise ship terminal Facility Security Officer (FSO) must—

(1) Maintain the TSP in the same or similar location as the FSP as described in §105.400(d);

(2) Have an accessible, complete copy of the TSP at the cruise ship terminal;

(3) Have a copy of the TSP available for inspection upon request by the Coast Guard;

(4) Maintain the TSP as sensitive security information (SSI) and protect it in accordance with 49 CFR part 1520; and

(5) Make a copy of the current Prohibited Items List (PIL) publicly available. The PIL and copies thereof are not SSI.

(c) *Content*. The TSP must include—

(1) A line diagram of the cruise ship terminal including—

(i) The physical boundaries of the terminal;

(ii) The location(s) where all persons intending to board a cruise ship, and all personal effects and baggage, are screened; and

(iii) The point(s) in the terminal beyond which no unscreened person may pass.

(2) The responsibilities of the owner or operator regarding the screening of persons, baggage, and personal effects;

(3) The procedure to obtain and maintain the PIL;

(4) The procedures used to comply with the requirements of §105.530 regarding qualifications of screeners;

(5) The procedures used to comply with the requirements of §105.535 regarding training of screeners;