

## § 105.125

the facility and are made available to the Coast Guard upon request:

(a) The approved Facility Security Plan (FSP), as well as any approved revisions or amendments thereto, and a letter of approval from the COTP dated within the last 5 years;

(b) The FSP submitted for approval and an acknowledgement letter from the COTP stating that the Coast Guard is currently reviewing the FSP submitted for approval, and that the facility may continue to operate so long as the facility remains in compliance with the submitted FSP; or

(c) For facilities operating under a Coast Guard-approved Alternative Security Program as provided in §105.140, a copy of the Alternative Security Program the facility is using, including a facility specific security assessment report generated under the Alternative Security Program, as specified in §101.120(b)(3) of this subchapter, and a letter signed by the facility owner or operator, stating which Alternative Security Program the facility is using and certifying that the facility is in full compliance with that program.

[USCG-2003-14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60541, Oct. 22, 2003]

## § 105.125 Noncompliance.

When a facility must temporarily deviate from the requirements of this part, the facility owner or operator must notify the cognizant COTP, and either suspend operations or request and receive permission from the COTP to continue operating.

[USCG-2003-14732, 68 FR 60541, Oct. 22, 2003]

## § 105.130 Waivers.

Any facility owner or operator may apply for a waiver of any requirement of this part that the facility owner or operator considers unnecessary in light of the nature or operating conditions of the facility, prior to operating. A request for a waiver must be submitted in writing with justification to the Commandant (CG-54) at 2100 Second St., SW., Washington, DC 20593. The Commandant (CG-54) may require the facility owner or operator to provide data for use in determining the validity of the requested waiver. The Commandant (CG-54) may grant, in writing,

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

a waiver with or without conditions only if the waiver will not reduce the overall security of the facility, its employees, visiting vessels, or ports.

[USCG-2003-14732, 68 FR 39322, July 1, 2003; 68 FR 41916, July 16, 2003; USCG-2008-0179, 73 FR 35009, June 19, 2008]

## § 105.135 Equivalentents.

For any measure required by this part, the facility owner or operator may propose an equivalent as provided in §101.130 of this subchapter.

## § 105.140 Alternative Security Program.

(a) A facility owner or operator may use an Alternative Security Program approved under §101.120 of this subchapter if:

(1) The Alternative Security Program is appropriate to that facility;

(2) The Alternative Security Program is implemented in its entirety.

(b) A facility owner or operator using an Alternative Security Program approved under §101.120 of this subchapter must complete and submit to the cognizant COTP a Facility Vulnerability and Security Measures Summary (Form CG-6025) in appendix A to part 105—Facility Vulnerability and Security (CG-6025).

## § 105.145 Maritime Security (MARSEC) Directive.

Each facility owner or operator subject to this part must comply with any instructions contained in a MARSEC Directive issued under §101.405 of this subchapter.

## § 105.150 Right to appeal.

Any person directly affected by a decision or action taken under this part, by or on behalf of the Coast Guard, may appeal as described in §101.420 of this subchapter.

## Subpart B—Facility Security Requirements

### § 105.200 Owner or operator.

(a) Each facility owner or operator must ensure that the facility operates in compliance with the requirements of this part.

(b) For each facility, the facility owner or operator must:

(1) Define the security organizational structure and provide each person exercising security duties and responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate, in writing, by name or by title, a Facility Security Officer (FSO) and identify how the officer can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of an FSP;

(5) Ensure that the facility operates in compliance with the approved FSP;

(6) Ensure that the TWIC program is properly implemented as set forth in this part, including:

(i) Ensuring that only individuals who hold a TWIC and are authorized to be in the secure area in accordance with the FSP are permitted to escort;

(ii) Identifying what action is to be taken by an escort, or other authorized individual, should individuals under escort engage in activities other than those for which escorted access was granted; and

(iii) Notifying facility employees, and passengers if applicable, of what parts of the facility are secure areas and public access areas, as applicable, and ensuring such areas are clearly marked.

(7) Ensure that restricted areas are controlled and TWIC provisions are coordinated, if applied to such restricted areas;

(8) Ensure that adequate coordination of security issues takes place between the facility and vessels that call on it, including the execution of a Declaration of Security (DoS) as required by this part;

(9) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility for visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with vessel operators in advance of a vessel's arrival. In coordinating such leave, facility owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations. The text of these treaties can

be found at <http://www.marad.dot.gov/Programs/treaties.html>;

(10) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level;

(11) Ensure security for unattended vessels moored at the facility;

(12) Ensure the report of all breaches of security and transportation security incidents to the National Response Center in accordance with part 101 of this chapter;

(13) Ensure consistency between security requirements and safety requirements;

(14) Inform facility personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;

(15) Ensure that protocols consistent with section 105.255(c) of this part, for dealing with individuals requiring access who report a lost, damaged, or stolen TWIC, or who have applied for and not yet received a TWIC, are in place; and

(16) If applicable, ensure that protocols consistent with §105.257 of this part, for dealing with newly hired employees who have applied for and not yet received a TWIC, are in place.

[USCG-2003-14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60541, Oct. 22, 2003; USCG-2006-24196, 72 FR 3582, Jan. 25, 2007]

#### **§ 105.205 Facility Security Officer (FSO).**

(a) *General.* (1) The FSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and responsibilities required of the FSO.

(2) The same person may serve as the FSO for more than one facility, provided the facilities are in the same COTP zone and are not more than 50 miles apart. If a person serves as the FSO for more than one facility, the name of each facility for which he or she is the FSO must be listed in the Facility Security Plan (FSP) of each facility for which or she is the FSO.