certifying that the OCS facility is in full compliance with that program.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003; USCG–2007–28915, 81 FR 57713, Aug. 23, 2016]

§ 106.120 Noncompliance.

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

[USCG–2003–14759, 68 FR 60558, Oct. 22, 2003]

§ 106.125 Waivers.

Any OCS facility owner or operator may apply for a waiver of any requirement of this part that the OCS facility owner or operator considers unnecessary in light of the nature or operating conditions of the OCS facility. A request for a waiver must be submitted in writing with justification to the cognizant District Commander. The cognizant District Commander may require the OCS facility owner or operator to provide additional data for use in determining the validity of the requested waiver. The cognizant District Commander may grant a waiver, in writing, with or without conditions only if the waiver will not reduce the overall security of the OCS facility, its personnel, or visiting vessels.

§ 106.130 Equivalents.

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

§ 106.135 Alternative Security Program.

An OCS facility owner or operator may use an Alternative Security Program approved under § 101.120 of this subchapter if:

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

(b) The OCS facility does not serve vessels on international voyages; and

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

§ 106.140 Maritime Security (MARSEC) Directive.

All OCS facility owners or operators subject to this part must comply with any instructions contained in a MARSEC Directive issued under § 101.405 of this subchapter.

§ 106.145 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—Outer Continental Shelf (OCS) Facility Security Requirements

§ 106.200 Owner or operator.

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

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

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

(2) Designate in writing, by name or title, a Company Security Officer (CSO) and a Facility Security Officer (FSO) for each OCS facility and identify how those officers 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 a Facility Security Plan (FSP);

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

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

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

(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.

(7) Ensure that adequate coordination of security issues takes place between OCS facilities and vessels, including the execution of a Declaration of Security (DoS) as required by this part;

(8) Ensure, within 12 hours of notification of an increase in MARSEC level, implementation of the additional security measures required by the FSP for the new MARSEC level;

(9) Ensure all breaches of security and security incidents are reported in accordance with the requirements in part 101 of this subchapter;

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

(11) Inform OCS 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;

(12) Ensure that protocols consistent with §101.550 of this subchapter, 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

(13) If applicable, ensure that protocols consistent with §106.262 of this part, for dealing with newly hired employees who have applied for and not yet received a TWIC, are in place.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003; USCG–2006–24196, 72 FR 3585, Jan. 25, 2007; USCG–2007–28915, 81 FR 57713, Aug. 23, 2016]

§ 106.205 Company Security Officer (CSO).

(a) *General.* (1) An OCS facility owner or operator may designate a single CSO for all its OCS facilities to which this part applies, or may designate more than one CSO, in which case the owner or operator must clearly identify the OCS facilities for which each CSO is responsible.

(2) A CSO may perform other duties within the owner's or operator's organization, including the duties of a Facility Security Officer, provided he or she is able to perform the duties and responsibilities required of the CSO.

(3) The CSO may delegate duties required by this part, but remains responsible for the performance of those duties.

(4) The CSO must maintain a TWIC.

(b) *Qualifications.* The CSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Security administration and organization of the OCS facility;

(2) OCS facility and vessel operations and conditions;

(3) OCS facility and vessel security measures including the meaning and consequential requirements of the different MARSEC Levels;

(4) Emergency preparedness and response and contingency planning;

(5) Security equipment and systems and their operational limitations;

(6) Methods of conducting audits, inspection, control, and monitoring; and

(7) Techniques for security training and education, including security measures and procedures.

(c) In addition to the knowledge and training in paragraph (b) of this section, the CSO must have general knowledge, through training or equivalent job experience, in the following, as appropriate:

(1) Relevant international conventions, codes, and recommendations;

(2) Relevant government legislation and regulations;

(3) Responsibilities and functions of other security organizations;

(4) Methodology of Facility Security Assessment.

(5) Methods of OCS facility security surveys and inspections;

(6) Handling sensitive security information (SSI) and security related communications;

(7) Knowledge of current security threats and patterns;

(8) Recognition and detection of dangerous substances and devices;

(9) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(10) Techniques used to circumvent security measures;

(11) Methods of physical screening and non-intrusive inspections; and