

(d) *MARSEC Level 3*. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

- (1) Cooperating with responders;
- (2) Switching on all lights;
- (3) Switching on all surveillance equipment capable of recording activities on, or in the vicinity of, the OCS facility;
- (4) Maximizing the length of time such surveillance equipment (if not already in use) can continue to record; or
- (5) Preparing for underwater inspection of the OCS facility.

§ 106.280 Security incident procedures.

For each MARSEC Level, the OCS facility owner or operator must ensure the Facility Security Officer (FSO) and OCS facility security personnel are able to:

- (a) Respond to security threats or breaches of security and maintain critical OCS facility and OCS facility-to-vessel interface operations;
- (b) Deny access to the OCS facility, except to those responding to an emergency;
- (c) Evacuate the OCS facility in case of security threats or breaches of security; and
- (d) Report security incidents as required in § 101.305 of this subchapter;
- (e) Brief all OCS facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and
- (f) Secure non-critical operations in order to focus response on critical operations.

Subpart C—Outer Continental Shelf (OCS) Facility Security Assessment (FSA)

§ 106.300 General.

(a) The Facility Security Assessment (FSA) is a written document that is based on the collection of background information, the completion of an on-scene survey and an analysis of that information.

(b) A single FSA may be performed and applied to more than one OCS facility to the extent they share physical characteristics, location, and operations.

(c) Third parties may be used in any aspect of the FSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a FSA must be able to draw upon expert assistance in the following areas, as appropriate:

- (1) Knowledge of current and anticipated security threats and patterns;
- (2) Recognition and detection of dangerous substances and devices;
- (3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
- (4) Recognition of techniques used to circumvent security measures;
- (5) Methods used to cause a security incident;
- (6) Effects of dangerous substances and devices on structures and essential services;
- (7) OCS facility security requirements;
- (8) OCS facility and vessel interface business practices;
- (9) Contingency planning, emergency preparedness and response;
- (10) Physical security requirements;
- (11) Radio and telecommunications systems, including computer systems and networks;
- (12) Marine or civil engineering; and
- (13) OCS facility and vessel operations.

§ 106.305 Facility Security Assessment (FSA) requirements.

(a) *Background*. The OCS facility owner or operator must ensure that the following background information, if applicable, is provided to the person or persons who will conduct the assessment:

- (1) The general layout of the OCS facility, including:
 - (i) The location of each access point to the OCS facility;
 - (ii) The number, reliability, and security duties of OCS facility personnel;
 - (iii) Security doors, barriers, and lighting;
 - (iv) The location of restricted areas;
 - (v) The emergency and stand-by equipment available to maintain essential services;
 - (vi) The essential maintenance equipment and storage areas;
 - (vii) Location of escape and evacuation routes and assembly stations; and
 - (viii) Existing security and safety equipment for protection of personnel;
- (2) Response procedures for fire or other emergency conditions;
- (3) Procedures for monitoring OCS facility and vessel personnel;
- (4) Procedures for controlling keys and other access prevention systems;
- (5) Response capability for security incidents;
- (6) Threat assessments, including the purpose and methodology of the

assessment, for the OCS facility's location;

(7) Previous reports on security needs; and

(8) Any other existing security procedures and systems, equipment, communications, and OCS facility personnel.

(b) *On-scene survey*. The OCS facility owner or operator must ensure that an on-scene survey of each OCS facility is conducted. The on-scene survey examines and evaluates existing OCS facility protective measures, procedures, and operations to verify or collect the information required in paragraph (a) of this section.

(c) *Analysis and recommendations*. In conducting the FSA, the OCS owner or operator must ensure that the Company Security Officer (CSO) analyzes the OCS facility background information and the on-scene survey, and considering the requirements of this part, provides recommendations to establish and prioritize the security measures that should be included in the FSP. The analysis must consider:

(1) Each vulnerability found during the on-scene survey, including but not limited to:

- (i) Access to the OCS facility;
- (ii) Structural integrity of the OCS facility;
- (iii) Existing security measures and procedures, including identification systems;
- (iv) Existing security measures and procedures relating to essential services;
- (v) Measures to protect radio and telecommunication equipment, including computer systems and networks;
- (vi) Existing agreements with private security companies;
- (vii) Any conflicting policies between safety and security measures and procedures;
- (viii) Any conflicting OCS facility operations and security duty assignments;
- (ix) Any deficiencies identified during daily operations or training and drills; and

(x) Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits.

(2) Possible security threats, including but not limited to:

- (i) Damage to or destruction of the OCS facility or of a vessel adjacent to the OCS facility;
- (ii) Smuggling dangerous substances and devices;
- (iii) Use of a vessel interfacing with the OCS facility to carry those intending to cause a security incident and their equipment;