KEY

VULNERABILITY CATEGORY:		
Physical Security	PHS	That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against terrorism, espionage, sabotage, damage, and theft.
Structural Integrity	STI	The design and material construction characteristics of piers, facilities, and associated structures.
Transportation Infrastructure	TRI	Infrastructure that may be exploited during an attack, other than utilities.
Utilities	UTI	The essential equipment and services that are vital to the operation of the facility.
Radio & Telecommunications	RAT	That part of security concerned with measures to protect radio and telecommunication equipment, including computer systems and networks.
Personnel Protection Systems	PPS	Equipment, Gear, or Systems designed to protect facility personnel (i.e. weapons, body armor).
Procedural Policies	PRP	Plans, Policies, and Procedures for specific operations.
Coordination and Information Sharing	CIS	The ability to coordinate and receive/share information with local/state/federal agencies and other commercial entities.
Preparedness	PRE	Implementation of Plans, Policies, and Procedures through Training, Drills, and Exercises conducted to improve security awareness, prevention, and response.

SECURITY MEASURES			
Access Control	ACC	Lighting	LIT
Barriers	BAR	Patrols	PAT
Cargo Control	CAC	Planning, Policies, & Procedures	PPP
Communications	COM	Redundancy	RED
Coordination	COR	Response	RES
Credentialing	CRE	Stand-off Distance	SOD
Detection	DET	Structural Hardening	STH
Guard Force	GUF	Surveillance	SUR
IT Security	ITS	Training	TRA
Inspections	INS	Vessels/Vehicles	VEV
Intelligence	INT		

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60543, Oct. 22, 2003]

PART 106—MARINE SECURITY: OUTER CONTINENTAL SHELF (OCS) FACILITIES

Subpart A—General

Sec.

Subpart B—Outer Continental Shelf (OCS) Facility Security Requirements

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

Subpart D—Outer Continental Shelf (OCS) Facility Security Plan (FSP)

AUTHORITY: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department Of Homeland Security Delegation No. 0170.1.

SOURCE: USCG–2003–14759, 68 FR 39345, July 1, 2003, unless otherwise noted.

Subpart A—General

§ 106.100 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

§ 106.105 Applicability.

(a) The requirements in this part apply to owners and operators of any fixed or floating facility, including MODUs not subject to part 104 of this subchapter, operating on the Outer Continental Shelf (OCS) of the United States for the purposes of engaging in the exploration, development, or production of oil, natural gas, or mineral resources that are regulated by 33 CFR subchapter N, that meet the following operating conditions:

(1) Hosts more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more;

(2) Produces greater than 100,000 barrels of oil per day; or

(3) Produces greater than 200 million cubic feet of natural gas per day.

(b) The TWIC requirements found in this part do not apply to mariners employed aboard vessels moored at U.S. OCS facilities only when they are working immediately adjacent to their vessels in the conduct of vessel activities.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended by USCG–2006–24196, 72 FR 55048, Sept. 28, 2007]

§ 106.110 Compliance dates.

(a) On or before December 31, 2003, OCS facility owners or operators must submit to the cognizant District Commander for each OCS facility—

(1) The Facility Security Plan described in subpart D of this part for review and approval; or

(2) If intending to operate under an approved Alternative Security Program, a letter signed by the OCS facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) On or before July 1, 2004, each OCS facility owner or operator must be operating in compliance with this part.

(c) OCS facilities built on or after July 1, 2004, must submit for approval an FSP 60 days prior to beginning operations.

(d) Persons required to obtain a TWIC under this part may enroll beginning after the date set by the Coast Guard in a Notice to be published in the FEDERAL REGISTER. This notice will be directed to all facilities and vessels within a specific COTP zone.

(e) Facility owners or operators must be operating in accordance with the TWIC provisions in this part by the date set by the Coast Guard in a Notice to be published in the FEDERAL REGISTER. This Notice will be published at least 90 days before compliance must begin, and will be directed to all facilities within a specific Captain of the Port zone, based on whether enrollment has been completed in that zone. Unless an earlier compliance date is specified in this manner, all facility

owner or operators will need to implement their TWIC provisions no later than April 15, 2009.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60557, Oct. 22, 2003; USCG–2006–24196, 72 FR 3585, Jan. 25, 2007; 73 FR 25565, May 7, 2008]

§ 106.115 Compliance documentation.

Each OCS facility owner or operator subject to this part must ensure before July 1, 2004, that copies of the following documentation are available at the OCS facility and are made available to the Coast Guard upon request:

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

(b) The FSP submitted for approval and current written acknowledgment from the cognizant District Commander, stating that the Coast Guard is currently reviewing the FSP submitted for approval and that the OCS facility may continue to operate so long as the OCS facility remains in compliance with the submitted FSP; or

(c) For OCS facilities operating under a Coast Guard-approved Alternative Security Program as provided in §106.135, a copy of the Alternative Security Program the OCS 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 OCS facility owner or operator, stating which Alternative Security Program the OCS facility is using and 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]

§ 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 part, 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 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 §106.260(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

(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]

§ 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

(12) Conducting and assessing security drills and exercises.

(13) Knowledge of TWIC requirements.

(d) *Responsibilities.* In addition to any other duties required by this part, for each OCS facility for which the CSO is responsible, the CSO must:

(1) Keep the OCS facility apprised of potential threats or other information relevant to its security;

(2) Ensure that a Facility Security Assessment (FSA) is carried out in compliance with this part;

(3) Ensure that a Facility Security Plan (FSP) is developed, approved, maintained, and implemented in compliance with this part;

(4) Ensure that the FSP is modified when necessary to comply with this part;

(5) Ensure that OCS facility security activities are audited in compliance with this part;

(6) Ensure the timely correction of problems identified by audits or inspections;

(7) Enhance security awareness and vigilance within the owner's or operator's organization;

(8) Ensure relevant personnel receive adequate security training in compliance with this part;

(9) Ensure communication and cooperation between the OCS facility and vessels that interface with it, in compliance with this part;

(10) Ensure consistency between security requirements and safety requirements in compliance with this part;

(11) Ensure that if a common FSP is prepared for more than one similar OCS facility, the FSP reflects any OCS facility specific characteristics; and

(12) Ensure compliance with an Alternative Security Program or equivalents approved under this subchapter, if appropriate.

(13) Ensure the TWIC program is being properly implemented.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003, as amended at 68 FR 60558, Oct. 22, 2003; USCG–2006–24196, 72 FR 3585, Jan. 25, 2007]

§ 106.210 OCS 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 of each such OCS facility.

(2) The same person may serve as the FSO for more than one OCS facility, provided the facilities are within a reasonable proximity to each other. If a person serves as the FSO for more than one OCS facility, the name of each OCS facility for which he or she is the FSO must be listed in the Facility Security Plan (FSP) of each OCS facility for which he or she is the FSO.

(3) The FSO may assign security duties to other OCS facility personnel; however, the FSO remains responsible for these duties.

(4) The FSO must maintain a TWIC.

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

(1) Those items listed in §106.205(b), and as appropriate §106.205(c), of this part;

(2) OCS facility layout;

(3) The FSP and related procedures; and

(4) Operation, testing and maintenance of security equipment and systems.

(c) *Responsibilities.* In addition to any other responsibilities specified elsewhere in this part, the FSO must, for each OCS facility for which he or she has been designated:

(1) Regularly inspect the OCS facility to ensure that security measures are maintained in compliance with this part;

(2) Ensure the maintenance of and supervision of the implementation of the FSP, and any amendments to the FSP, in compliance with this part;

(3) Ensure the coordination and handling of stores and industrial supplies in compliance with this part;

(4) Where applicable, propose modifications to the FSP to the Company Security Officer (CSO);

(5) Ensure that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions;

(6) Ensure security awareness and vigilance on board the OCS facility;

(7) Ensure adequate security training for OCS facility personnel in compliance with this part;

(8) Ensure the reporting and recording of all security incidents in compliance with this part;

(9) Ensure the coordinated implementation of the FSP with the CSO;

(10) Ensure that security equipment is properly operated, tested, calibrated and maintained in compliance with this part;

(11) Ensure consistency between security requirements and the proper treatment of OCS facility personnel affected by those requirements;

(12) Ensure that occurrences that threaten the security of the OCS facility are recorded and reported to the CSO;

(13) Ensure that when changes in the MARSEC Level are attained they are recorded and reported to the CSO, OCS facility owner or operator, and the cognizant District Commander; and

(14) Have prompt access to a copy of the FSA, along with an approved copy of the FSP.

(15) Ensure the TWIC program is properly implemented.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended by USCG–2006–24196, 72 FR 3585, Jan. 25, 2007

§106.215 Company or OCS facility personnel with security duties.

Company and OCS facility personnel responsible for security duties must maintain a TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:

(a) Knowledge of current and anticipated security threats and patterns.

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

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

(d) Recognition of techniques used to circumvent security measures;

(e) Security related communications;

(f) Knowledge of emergency procedures and contingency plans;

(g) Operation of security equipment and systems;

(h) Testing, calibration, and maintenance of security equipment and systems;

(i) Inspection, control, and monitoring techniques;

(j) Methods of physical screenings of persons, personal effects, stores and industrial supplies;

(k) Familiarity with all relevant aspects of the TWIC program and how to carry them out;

(l) Relevant provisions of the Facility Security Plan (FSP); and

(m) The meaning and the consequential requirements of the different MARSEC Levels.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003, as amended by USCG–2006–24196, 72 FR 3586, Jan. 25, 2007]

§ 106.220 Security training for all other OCS facility personnel.

All other OCS facility personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge, through training or equivalent job experience, of the following, as appropriate:

(a) Relevant provisions of the Facility Security Plan (FSP);

(b) The meaning and the consequential requirements of the different MARSEC Levels including emergency procedures and contingency plans;

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

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

(e) Recognition of techniques used to circumvent security measures.

(f) Familiarity with all relevant aspects of the TWIC program and how to carry them out.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003; USCG–2006–24196, 72 FR 3586, Jan. 25, 2007]

§ 106.225 Drill and exercise requirements.

(a) *General.* (1) Drills and exercises must test the proficiency of facility personnel in assigned security duties at all MARSEC Levels and the effective implementation of the Facility Security Plan (FSP). They must enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the FSP as the result of an increase in the MARSEC Level, provided the FSO reports attainment to the cognizant District Commander.

(b) *Drills.* (1) From the date of the FSP approval, the FSO must ensure that at least one security drill is conducted every 3 months. Security drills may be held in conjunction with non-security drills, where appropriate.

(2) Drills must test individual elements of the FSP, including response to security threats and incidents. Drills should take into account the types of operations of the OCS facility, OCS facility personnel changes, the types of vessels calling at the OCS facility, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of appropriate authorities.

(3) If a vessel is conducting operations with the OCS facility on the date the OCS facility has planned to conduct any drills, the OCS facility may include, but cannot require, the vessel or vessel personnel to participate in the OCS facility's scheduled drill.

(c) *Exercises.* (1) From the date of the FSP approval, exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be:

(i) Full scale or live;

(ii) Tabletop simulation;

(iii) Combined with other appropriate exercises held; or

(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be facility-specific or part of a cooperative exercise program.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the Facility Security Plan and must include substantial and active participation of relevant company and OCS facility personnel, and may include governmental authorities and vessels depending on the scope and the nature of the exercise.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

§ 106.230 OCS facility recordkeeping requirements.

(a) Unless otherwise specified in this section, the Facility Security Officer (FSO) must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized access, deletion, destruction,

amendment, and disclosure. The following records must be kept:

(1) *Training.* For training under §106.215, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) *Drills and exercises.* For each drill or exercise, the date held, a description of the drill or exercise, a list of participants, and any best practices or lessons learned which may improve the FSP;

(3) *Incidents and breaches of security.* Date and time of occurrence, location within the OCS facility, a description of the incident or breach, the identity of the individual to whom it was reported, and a description of the response;

(4) *Changes in MARSEC Levels.* Date and time of the notification received, and the time of compliance with additional requirements;

(5) *Maintenance, calibration, and testing of security equipment.* For each occurrence of maintenance, calibration, and testing, record the date and time, and the specific security equipment involved;

(6) *Security threats.* Date and time of occurrence, how the threat was communicated, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response;

(7) *Declaration of Security (DoS).* A copy of each DoS for at least 90 days after the end of its effective period; and

(8) *Annual audit of the Facility Security Plan (FSP).* For each annual audit, a letter certified by the FSO stating the date the audit was conducted.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

§106.235 Maritime Security (MARSEC) Level coordination and implementation.

(a) The OCS facility owner or operator must ensure the OCS facility operates in compliance with the security requirements in this part for the MARSEC Level in effect for the OCS facility.

(b) When notified of an increase in the MARSEC Level, the OCS facility owner or operator must ensure:

(1) Vessels conducting operations with the OCS facility and vessels scheduled to arrive at the OCS facility within 96 hours of the MARSEC Level change are notified of the new MARSEC Level and the Declaration of Security (DoS), if applicable, is revised as necessary;

(2) The OCS facility complies with the required additional security measures within 12 hours; and

(3) The OCS facility reports compliance or noncompliance to the cognizant District Commander.

(c) For MARSEC Levels 2 and 3, the Facility Security Officer (FSO) must inform all OCS facility personnel about identified threats, emphasize reporting procedures, and stress the need for increased vigilance.

(d) An OCS facility owner or operator whose facility is not in compliance with the requirements of this section must so inform the cognizant District Commander and obtain approval prior to interfacing with another vessel or prior to continuing operations.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003]

§106.240 Communications.

(a) The Facility Security Officer (FSO) must have a means to effectively notify OCS facility personnel of changes in security conditions at the OCS facility.

(b) Communication systems and procedures must allow effective and continuous communications between the OCS facility security personnel, vessels interfacing with the OCS facility, the cognizant District Commander, and national and local authorities with security responsibilities.

(c) Facility communications systems must have a backup means for both internal and external communications.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003]

§106.245 Procedures for interfacing with vessels.

The OCS facility owner or operator must ensure that there are measures for interfacing with vessels at all MARSEC Levels.

§ 106.250 Declaration of Security (DoS).

(a) Each OCS facility owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from vessels.

(b) At MARSEC Level 1, owners or operators of OCS facilities interfacing with a manned vessel carrying Certain Dangerous Cargoes, in bulk, must:

(1) Prior to the arrival of a vessel to the OCS facility, ensure the Facility Security Officer (FSO) and Master, Vessel Security Officer (VSO), or their designated representatives coordinate security needs and procedures, and agree upon the contents of a DoS for the period of time the vessel is at the OCS facility; and

(2) Upon the arrival of the vessel at the OCS facility, the FSO and Master, VSO, or their designated representatives, must sign the written DoS.

(c) Neither the OCS facility nor the vessel may embark or disembark personnel, or transfer stores or industrial supplies until the DoS has been signed.

(d) At MARSEC Levels 2 and 3, the FSOs of OCS facilities interfacing with manned vessels subject to part 104 of this chapter, or their designated representatives, must sign and implement DoSs as required in paragraphs (b)(1) and (b)(2) of this section.

(e) At MARSEC Levels 1 and 2, FSOs of OCS facilities that frequently interface with the same vessel may implement a continuing DoS for multiple visits, provided that:

(1) The DoS is valid for a specific MARSEC Level;

(2) The effective period at MARSEC Level 1 does not exceed 90 days; and

(3) The effective period at MARSEC Level 2 does not exceed 30 days.

(f) When the MARSEC Level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed in accordance with this section.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

§ 106.255 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.

(b) Security systems must be regularly tested in accordance with the manufacturers' recommendations; noted deficiencies corrected promptly; and the results recorded as required in § 106.230(b)(5) of this part.

(c) The Facility Security Plan (FSP) must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 106.260 Security measures for access control.

(a) *General.* The OCS facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, or the OCS facility;

(2) Secure dangerous substances and devices that are authorized by the OCS facility owner or operator to be on board;

(3) Control access to the OCS facility; and

(4) Prevent an unescorted individual from entering the OCS facility unless the individual holds a duly issued TWIC and is authorized to be on the OCS facility.

(b) The OCS facility owner or operator must ensure that the following are specified:

(1) All locations providing means of access to the OCS facility where access restrictions or prohibitions are applied for each security level to prevent unauthorized access, including those points where TWIC access control procedures will be applied;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them;

(3) The means used to establish the identity of individuals not in possession of a TWIC and the means by which they will be allowed access to the OCS facility; and

(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level.

(c) The OCS facility owner or operator must ensure that a TWIC program is implemented as follows:

(1) All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with §101.514 of this subchapter. Inspection must include:

(i) A match of the photo on the TWIC to the individual presenting the TWIC;

(ii) Verification that the TWIC has not expired; and

(iii) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

(2) If an individual cannot present a TWIC because it has been lost, damaged or stolen, and he or she has previously been granted unescorted access to the facility and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than seven consecutive calendar days if:

(i) The individual has reported the TWIC as lost, damaged or stolen to TSA as required in 49 CFR 1572.19(f);

(ii) The individual can present another identification credential that meets the requirements of §101.515 of this subchapter; and

(iii) There are no other suspicious circumstances associated with the individual's claim of loss or theft.

(3) If an individual cannot present his or her TWIC for any other reason than outlined in paragraph (c)(2) of this section, he or she may not be granted unescorted access to the secure area. The individual must be under escort, as that term is defined in part 101 of this subchapter, at all times when inside of a secure area.

(4) With the exception of persons granted access according to paragraph (c)(2) of this section, all persons granted unescorted access to secure areas of the facility must be able to produce his or her TWIC upon request.

(5) There must be disciplinary measures in place to prevent fraud and abuse.

(6) The facility's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of vessels or other transportation conveyances that use the facility.

(d) If the OCS facility owner or operator uses a separate identification system, ensure that it is coordinated with identification and TWIC systems in place on vessels conducting operations with the OCS facility.

(e) The OCS facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(f) *MARSEC Level 1.* The OCS facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Implement TWIC as set out in paragraph (c) of this section.

(2) Screen persons and personal effects going aboard the OCS facility for dangerous substances and devices at the rate specified in the approved FSP;

(3) Conspicuously post signs that describe security measures currently in effect and clearly stating that:

(i) Boarding an OCS facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to be on board;

(4) Check the identification of any person seeking to board the OCS facility, including OCS facility employees, passengers and crews of vessels interfacing with the OCS facility, vendors, and visitors and ensure that non-TWIC holders are denied unescorted access to the OCS facility;

(5) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of OCS facility personnel or a law enforcement officer, to establish his or her identity in accordance with this part or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(6) Deter unauthorized access to the OCS facility;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Lock or otherwise prevent access to unattended spaces that adjoin areas to which OCS facility personnel and visitors have access;

(9) Ensure OCS facility personnel are not required to engage in or be subjected to screening, of the person or of personal effects, by other OCS facility personnel, unless security clearly requires it;

(10) Provide a designated secure area on board, or in liaison with a vessel interfacing with the OCS facility, for conducting inspections and screening of people and their personal effects; and

(11) Respond to the presence of unauthorized persons on board.

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

(1) Increasing the frequency and detail of screening of people and personal effects embarking onto the OCS facility as specified for MARSEC Level 2 in the approved FSP;

(2) Assigning additional personnel to patrol deck areas during periods of reduced OCS facility operations to deter unauthorized access;

(3) Limiting the number of access points to the OCS facility by closing and securing some access points; or

(4) Deterring waterside access to the OCS facility, which may include, providing boat patrols.

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

(1) Screening all persons and personal effects for dangerous substances and devices;

(2) Being prepared to cooperate with responders;

(3) Limiting access to the OCS facility to a single, controlled access point;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending embarkation and/or disembarkation of personnel;

(6) Suspending the loading of stores or industrial supplies;

(7) Evacuating the OCS facility; or

(8) Preparing for a full or partial search of the OCS facility.

[USCG–2006–24196, 72 FR 3586, Jan. 25, 2007]

§ 106.262 Security measures for newly-hired employees.

(a) Newly-hired OCS facility employees may be granted entry to secure areas of the OCS facility for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements in paragraph (b) of this section are met, and provided that the new hire is accompanied by an individual with a TWIC while within the secure areas of the OCS facility. If TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend access to secure areas for another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. The Coast Guard will issue guidance for use in making these determinations.

(b) Newly-hired OCS facility employees may be granted the access provided for in paragraph (a) of this section if:

(1) The new hire has applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process, paying the user fee, and is not currently engaged in a waiver or appeal process. The OCS facility owner or operator or Facility Security Officer (FSO) must have th enew hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC;

(2) The OCS facility owner or operator or the FSO enters the following information on the new hire into the Coast Guard's Homeport Web site (*http://homeport.uscg.mil*):

(i) Full legal name, including middle name if one exists;

(ii) Date of birth;

(iii) Social security number (optional);

(iv) Employer name and 24 hour contact information; and

(v) Date of TWIC enrollment.

(3) The new hire presents an identification credential that meets the requirements of §101.515 of this subchapter;

(4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the OCS facility owner or operator or FSO have not been informed by the cognizant COTP that the individual poses a security threat; and

(5) There would be an adverse impact to OCS facility operations if the new hire is not allowed access.

(c) This section does not apply to any individual being hired as a Company Security Officer or FSO, or any individual being hired to perform OCS facility security duties.

(d) The new hire may not begin working at the OCS facility under the provisions of this section until the owner, operator, or FSO receives notification, via Homeport or some other means, the new hire has passed an initial name check.

[USCG–2006–24196, 72 FR 3587, Jan. 25, 2007]

§106.265 Security measures for restricted areas.

(a) *General.* The OCS facility owner or operator must ensure the designation of restricted areas in order to:

(1) Prevent or deter unauthorized access;

(2) Protect persons authorized to be in the OCS facility;

(3) Protect the OCS facility;

(4) Protect vessels using and serving the OCS facility;

(5) Protect sensitive security areas within the OCS facility;

(6) Protect security and surveillance equipment and systems; and

(7) Protect stores and industrial supplies from tampering.

(b) *Designation of restricted areas.* The OCS facility owner or operator must ensure restricted areas are designated within the OCS facility. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The OCS facility owner or operator may designate the entire OCS facility as a restricted area. Restricted areas must include, as appropriate:

(1) Areas containing sensitive security information;

(2) Areas containing security and surveillance equipment and systems and their controls, and lighting system controls; and

(3) Areas containing critical OCS facility infrastructure equipment, including:

(i) Water supplies;

(ii) Telecommunications;

(iii) Power distribution system;

(iv) Access points for ventilation and air-conditioning systems;

(v) Manufacturing areas and control rooms;

(vi) Areas designated for loading, unloading or storage of stores and industrial supplies; and

(vii) Areas containing hazardous materials.

(c) The OCS facility owner or operator must ensure that the Facility Security Plan (FSP) includes measures for restricted areas to:

(1) Identify which OCS facility personnel are authorized to have access;

(2) Determine which persons other than OCS facility personnel are authorized to have access;

(3) Determine the conditions under which that access may take place;

(4) Define the extent of any restricted area; and

(5) Define the times when access restrictions apply.

(d) *MARSEC Level 1.* At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

(1) Restricting access to only authorized personnel;

(2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;

(3) Verifying the identification and authorization of all persons seeking entry;

(4) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry

to or movement within restricted areas; or

(5) Designating temporary restricted areas to accommodate OCS facility operations. If temporary restricted areas are designated, the FSP must include security requirements to conduct a security sweep of the designated temporary restricted areas both before and after the area has been established.

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

(1) Enhancing the effectiveness of the barriers surrounding restricted areas, for example, by the use of patrols or automatic intrusion detection devices;

(2) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;

(3) Further restricting access to the restricted areas and movements and storage within them;

(4) Using continuously monitored and recorded surveillance equipment;

(5) Increasing the number and frequency of patrols, including the use of waterborne patrols; or

(6) Restricting access to areas adjacent to the restricted areas.

(f) *MARSEC Level 3.* In addition to the security measures required 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 their approved FSP. These additional security measures may include:

(1) Restricting access to additional areas;

(2) Prohibiting access to restricted areas; or

(3) Searching restricted areas as part of a security sweep of all or part of the OCS facility.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

§ 106.270 Security measures for delivery of stores and industrial supplies.

(a) *General.* The OCS facility owner or operator must ensure that security measures relating to the delivery of stores or industrial supplies to the OCS facility are implemented to:

(1) Check stores or industrial supplies for package integrity;

(2) Prevent stores or industrial supplies from being accepted without inspection;

(3) Deter tampering; and

(4) Prevent stores and industrial supplies from being accepted unless ordered. For any vessels that routinely use an OCS facility, an OCS facility owner or operator may establish and implement standing arrangements between the OCS facility, its suppliers, and any vessel delivering stores or industrial supplies regarding notification and the timing of deliveries and their documentation.

(b) *MARSEC Level 1.* At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of measures to:

(1) Inspect stores or industrial supplies before being accepted; and

(2) Check that stores or industrial supplies match the order prior to being brought on board.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved Facility Security Plan (FSP). These additional security measures may include:

(1) Intensifying inspection of the stores or industrial supplies during delivery; or

(2) Checking stores or industrial supplies prior to receiving them on board.

(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) Checking all OCS facility stores or industrial supplies more extensively;

(2) Restricting or suspending delivery of stores or industrial supplies; or

(3) Refusing to accept stores or industrial supplies on board.

§ 106.275 Security measures for monitoring.

(a) *General.* (1) The OCS facility owner or operator must ensure the implementation of security measures in this section and have the capability to continuously monitor, through a combination of lighting, watchkeepers, security guards, deck watches, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment as specified in their approved Facility Security Plan (FSP), the:

(i) OCS facility;

(ii) Restricted areas on board the OCS facility; and

(iii) The area surrounding the OCS facility.

(2) The following must be considered when establishing the appropriate level and location of lighting:

(i) OCS facility personnel should be able to detect activities on and around OCS facilities;

(ii) Coverage should facilitate personnel identification at access points; and

(iii) Lighting effects, such as glare, and their impact on safety, navigation, and other security activities.

(b) *MARSEC Level 1.* At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of security measures, which may be implemented in coordination with a vessel interfacing with the OCS facility, to:

(1) Monitor the OCS facility, particularly OCS facility access points and restricted areas;

(2) Be able to conduct emergency searches of the OCS facility;

(3) Ensure that equipment or system failures or malfunctions are identified and corrected;

(4) Ensure that any automatic intrusion detection device, sets off an audible or visual alarm, or both, at a location that is continuously attended or monitored; and

(5) Light deck and OCS facility access points during the period between sunset and sunrise and periods of limited visibility sufficiently to allow visual identification of persons seeking access to the OCS facility.

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

(1) Increasing the frequency and detail of security patrols;

(2) Using (if not already in use) or increasing the use of security and surveillance equipment;

(3) Assigning additional personnel as security lookouts; or

(4) Coordinating with boat patrols, when provided.

(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.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

§ 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.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003]

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;

(iv) Use of a vessel interfacing with the OCS facility as a weapon or as a means to cause damage or destruction; and

(v) Effects of a nuclear, biological, radiological, explosive, or chemical attack to the OCS facility's shoreside support system;

(3) Threat assessments by Government agencies;

(4) Vulnerabilities, including human factors, in the OCS facility's infrastructure, policies and procedures;

(5) Any particular aspects of the OCS facility, including the vessels that interface with the OCS facility, which make it likely to be the target of an attack;

(6) Likely consequences, in terms of loss of life, damage to property, or economic disruption, of an attack on or at the OCS facility; and

(7) Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

(d) *FSA Report.* (1) The OCS facility owner or operator must ensure that a written FSA report is prepared and included as a part of the FSP. The report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) A description of existing security measures, including inspection, control 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 OCS 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 OCS facility.

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

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(v) Radio and telecommunication systems, including computer systems and networks; and

(vi) Essential services.

(3) The FSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) OCS facility personnel;

(ii) Visitors, vendors, repair technicians, vessel personnel, etc.;

(iii) OCS facility stores;

(iv) Any security communication and surveillance systems; and

(v) Any other 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 personnel duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on 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 OCS facility measures and operations, including—

(i) Ensuring performance of all security duties;

(ii) Controlling access to the OCS facility through the use of identification systems or otherwise;

(iii) Controlling the embarkation of OCS facility personnel and other persons and their effects (including personal effects and baggage, whether accompanied or unaccompanied);

(iv) Supervising the delivery of stores and industrial supplies;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring deck areas and areas surrounding the OCS facility; 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–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

§ 106.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan (FSP) required in § 106.410 of this part.

(b) An OCS facility owner or operator may generate and submit a report that contains the FSA for more than one OCS facility subject to this part, to the extent that they share similarities in physical characteristics, location and operations.

(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–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

Subpart D—Outer Continental Shelf (OCS) Facility Security Plan (FSP)

§ 106.400 General.

(a) The OCS facility owner or operator must ensure the FSO develops and implements a Facility Security Plan (FSP) for each OCS facility for which he or she is designated as FSO. The FSP:

(1) Must identify the FSO by name or 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 OCS facility to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the cognizant District Commander.

(b) The FSP must be submitted for approval to the cognizant District Commander in a written or electronic format in a manner prescribed by the cognizant District Commander.

(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.

§ 106.405 Format and content of the Facility Security Plan (FSP).

(a) An OCS 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 this paragraph, the OCS facility owner or operator must ensure that the FSP contains an index identifying the location of each of the following sections:

(1) Security organization of the OCS 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;

(11) Security measures for restricted areas;

(12) Security measures for delivery of stores and industrial supplies;

(13) Security measures for monitoring;

(14) Security incident procedures;

(15) Audits and FSP amendments; and

(16) Facility Security Assessment (FSA) report.

(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.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003, as amended by USCG–2006–24196, 72 FR 3587, Jan. 25, 2007]

§ 106.410 Submission and approval.

(a) On or before December 31, 2003, the owner or operator of each OCS facility currently in operation must either:

(1) Submit one copy of the Facility Security Plan (FSP) for review and approval to the cognizant District Commander and a letter certifying that the FSP meets the applicable requirements of this part; or

(2) If intending to operate under an Approved Security Program, submit a letter signed by the OCS facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) Owners or operators of OCS 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 or by December 31, 2003, whichever is later.

(c) The cognizant District Commander 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 OCS facility where they share similarities in physical characteristics, location, and operations.

(e) Each OCS facility owner or operator that submits one FSP to cover two or more OCS facilities of similar design, location, and operation must address OCS facility-specific information that includes the physical and operational characteristics of each OCS facility.

(f) An FSP that is approved by the cognizant District Commander is valid for 5 years from the date of its approval. The cognizant District Commander will issue an approval letter, as indicated in § 106.115 of this part.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

§ 106.415 Amendment and audit.

(a) *Amendments.* (1) Amendments to a Facility Security Plan (FSP) that are approved by the cognizant District Commander may be initiated by:

(i) The OCS facility owner or operator; or

(ii) The cognizant District Commander, upon a determination that an amendment is needed to maintain the OCS facility's security. The cognizant District Commander will give the OCS facility owner or operator written notice and request that the OCS facility owner or operator propose amendments addressing any matters specified in the notice. The OCS facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the OCS facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the cognizant District Commander.

(2) Proposed amendments must be sent to the cognizant District Commander. If initiated by the OCS facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant District Commander allows a shorter period. The cognizant District Commander will approve or disapprove the proposed amendment in accordance with §106.410 of this subpart.

(3) Nothing in this section should be construed as limiting the OCS 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 District Commander 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 the owner or operator has changed, the Facility Security Officer (FSO) must amend the Facility Security Plan (FSP) to include the name and contact information of the new OCS facility owner(s) or operator(s) and submit the affected portion of the FSP for review and approval in accordance with §106.410 of 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) If there is a change in ownership or operations of the OCS facility, or if there have been modifications to the OCS facility, the FSP must be audited 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 OCS facility may be limited to those sections of the FSP affected by the OCS facility modifications.

(4) Unless impracticable due to the size and nature of the company or the OCS facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must:

(i) Have knowledge of methods of conducting audits and inspections, and 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 an amendment of either the Facility Security Assessment (FSA) or FSP, the FSO must submit, in accordance with §106.410 of this subpart, the amendments to the cognizant District Commander 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–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60559, Oct. 22, 2003]

PART 107—NATIONAL VESSEL AND FACILITY CONTROL MEASURES AND LIMITED ACCESS AREAS

Subpart A [Reserved]

Subpart B—Unauthorized Entry Into Cuban Territorial Waters

Sec.