§ 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.