

§ 105.250

(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.

(g) A copy of all currently valid continuing DoSs must be kept with the Facility Security Plan.

(h) The COTP may require, at any time, at any MARSEC Level, any facility subject to this part to implement a DoS with the VSO prior to any vessel-to-facility interface when he or she deems it necessary.

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

§ 105.250 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 § 105.225 of this subpart.

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

§ 105.255 Security measures for access control.

(a) *General.* The 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, facilities, or ports;

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

(3) Control access to the facility; and

(4) Prevent an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued

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

TWIC and is authorized to be in the area.

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

(1) The locations where restrictions or prohibitions that prevent unauthorized access are applied for each MARSEC Level, including those points where TWIC access control provisions will be applied. Each location allowing means of access to the facility must be addressed;

(2) The types of restrictions or prohibitions 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, in accordance with § 101.515 of this subchapter, and procedures for escorting them;

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

(5) The locations where persons, personal effects and vehicle screenings are to be conducted. The designated screening areas should be covered to provide for continuous operations regardless of the weather conditions.

(c) The 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 7 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);