

in bulk, must comply with the following:

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

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

(c) Neither the facility nor the vessel may embark or disembark passengers, nor transfer cargo or vessel stores until the DoS has been signed and implemented.

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

(e) At MARSEC Levels 1 and 2, FSOs of 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.

(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 main-

tained 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 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