and the specific security equipment involved;

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

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

(b) **Annual audit of the FSP.** For each annual audit, a letter certified by the FSO stating the date the audit was completed.

(c) Any record required by this part must be protected from unauthorized access or disclosure.


**§ 105.230 Maritime Security (MARSEC) Level coordination and implementation.**

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

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

(1) Vessels moored to the facility and vessels scheduled to arrive at the facility within 96 hours of the MARSEC Level change are notified of the new MARSEC Level and the Declaration of Security is revised as necessary;

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

(3) The facility reports compliance or noncompliance to the COTP.

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

(d) An owner or operator whose facility is not in compliance with the requirements of this section, must inform the COTP and obtain approval prior to interfacing with a vessel or continuing operations.

(e) At MARSEC Level 3, in addition to the requirements in this part, a facility owner or operator may be required to implement additional measures, pursuant to 33 CFR part 6, 160, or 165, as appropriate, which may include but are not limited to:

(1) Use of waterborne security patrol;

(2) Use of armed security personnel to control access to the facility and to deter, to the maximum extent practical, a transportation security incident; and

(3) Examination of piers, wharves, and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats.

**§ 105.235 Communications.**

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

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

(c) At each active facility access point, provide a means of contacting police, security control, or an emergency operations center, by telephones, cellular phones, and/or portable radios, or other equivalent means.

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

**§ 105.240 Procedures for interfacing with vessels.**

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

**§ 105.245 Declaration of Security (DoS).**

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

(b) At MARSEC Level 1, a facility receiving a cruise ship or a manned vessel carrying Certain Dangerous Cargo,
Coast Guard, DHS

§ 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

§ 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 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