

33 CFR
Navigation and Navigable Waters
CHAPTER I
COAST GUARD, DEPARTMENT OF
HOMELAND SECURITY
SUBCHAPTER H -- MARITIME SECURITY

PART 105—MARITIME SECURITY:
FACILITIES

Subpart A-General

Sec.

- [105.100 Definitions.](#)
- [105.105 Applicability.](#)
- [105.106 Public access areas.](#)
- [105.110 Exemptions.](#)
- [105.115 Compliance dates.](#)
- [105.120 Compliance documentation.](#)
- [105.125 Noncompliance.](#)
- [105.130 Waivers.](#)
- [105.135 Equivalents.](#)
- [105.140 Alternative Security Program.](#)
- [105.145 Maritime Security \(MARSEC\) Directive.](#)
- [105.150 Right to appeal.](#)

Subpart B -- Facility Security Requirements

- [105.200 Owner or operator.](#)
- [105.205 Facility Security Officer \(FSO\).](#)
- [105.210 Facility personnel with security duties.](#)
- [105.215 Security training for all other facility personnel.](#)
- [105.220 Drill and exercise requirements.](#)
- [105.225 Facility recordkeeping requirements.](#)
- [105.230 Maritime Security \(MARSEC\) Level coordination and implementation.](#)
- [105.235 Communications.](#)
- [105.240 Procedures for interfacing with vessels.](#)
- [105.245 Declaration of Security \(DoS\).](#)
- [105.250 Security systems and equipment maintenance.](#)
- [105.255 Security measures for access control.](#)
- [105.260 Security measures for restricted areas.](#)
- [105.265 Security measures for handling cargo.](#)
- [105.270 Security measures for delivery of vessel stores and bunkers.](#)
- [105.275 Security measures for monitoring.](#)
- [105.280 Security incident procedures.](#)
- [105.285 Additional requirements -- passenger and ferry facilities.](#)
- [105.290 Additional requirements -- cruise ship terminals.](#)
- [105.295 Additional requirements -- Certain Dangerous Cargo \(CDC\) facilities.](#)
- [105.296 Additional requirements -- barge fleeing facilities.](#)

Subpart C -- Facility Security Assessment (FSA)

- [105.300 General.](#)
- [105.305 Facility Security Assessment \(FSA\) requirements.](#)
- [105.310 Submission requirements.](#)

Subpart D -- Facility Security Plan (FSP)

- [105.400 General.](#)
- [105.405 Format and content of the Facility Security Plan \(FSP\).](#)
- [105.410 Submission and approval.](#)
- [105.415 Amendment and audit.](#)
- [Appendix A to part 105 -- Facility Vulnerability and Security Measure Summary \(CG-6025\).](#)

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70103; 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-2003-14732, [68 FR 39322](#), July 1, 2003, unless otherwise noted.

Subpart A—General

§ 105.100 Definitions.

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

§ 105.105 Applicability.

(a) The requirements in this part apply to the owner or operator of any U.S.:

(1) Facility subject to 33 CFR parts 126, 127, or 154;

(2) Facility that receives vessels certificated to carry more than 150 passengers, except those vessels not carrying and not embarking or disembarking passengers at the facility;

(3) Facility that receives vessels subject to the International Convention for Safety of Life at Sea, 1974, chapter XI;

(4) Facility that receives foreign cargo vessels greater than 100 gross register tons;

(5) Facility that receives U.S. cargo vessels, greater than 100 gross register tons, subject to 46 CFR chapter I, subchapter I, except for those facilities that receive only commercial fishing vessels inspected under 46 CFR part 105; or

(6) Barge fleeing facility that receives barges carrying, in bulk, cargoes regulated by 46 CFR chapter I, subchapters D or O, or Certain Dangerous Cargoes.

(b) An owner or operator of any facility not covered in paragraph (a) of this section is subject to parts 101 through 103 of this subchapter.

(c) This part does not apply to the owner or operator of the following U.S. facilities:

(1) A facility owned or operated by the U.S. that is used primarily for military purposes.

(2) An oil and natural gas production, exploration, or development facility regulated by 33 CFR parts 126 or 154 if:

(i) The facility is engaged solely in the exploration, development, or production of oil and natural gas; and

(ii) The facility does not meet or exceed the operating conditions in §106.105 of this subchapter;

(3) A facility that supports the production, exploration, or development of oil and natural gas regulated by 33 CFR parts 126 or 154 if:

(i) **The facility is engaged solely in the support of exploration, development, or production of oil and natural gas and transports or stores quantities of hazardous materials that do not meet or exceed those specified in 49 CFR 172.800(b)(1) through (b)(6); or**

(ii) The facility stores less than 42,000 gallons of cargo regulated by 33 CFR part 154;

(4) A mobile facility regulated by 33 CFR part 154; or

(5) An isolated facility that receives materials regulated by 33 CFR parts 126 or 154 by vessel due to the lack of road access to the facility and does not distribute the material through secondary marine transfers.

§ 105.106 Public access areas.

(a) **A facility serving ferries or passenger vessels certificated to carry more than 150 passengers, other than cruise ships, may designate an area within the facility as a public access area.**

(b) A public access area is a defined space within a facility that is open to all persons and provides **pedestrian** access through the facility from public thoroughfares to the vessel.

§ 105.110 Exemptions.

(a) An owner or operator of any barge fleeting facility subject to this part is exempt from complying with §105.265, Security measures for handling cargo; and §105.270, Security measures for delivery of vessel stores and bunkers.

(b) **A public access area designated under § 105.106 is exempt from the requirements for screening of persons, baggage, and personal effects and identification of persons in § 105.255(c), (e)(1), (e)(3), (f)(1), and (g)(1) and § 105.285(a)(1).**

(c) **An owner or operator of any general shipyard facility as defined in § 101.105 is exempt from the requirements of this part unless the facility:**

(1) **Is subject to parts 126, 127, or 154 of this chapter; or**

(2) **Provides any other service to vessels subject to part 104 of this subchapter not related to construction, repair, rehabilitation, refurbishment, or rebuilding.**

(d) **Public access facility.** (1) The COTP may exempt a public access facility from the requirements of this part, including establishing

conditions for which such an exemption is granted, to ensure that adequate security is maintained.

(2) **The owner or operator of any public access facility exempted under this section must:**

(i) **Comply with any COTP conditions for the exemption; and**

(ii) **Ensure that the cognizant COTP has the appropriate information for contacting the individual with security responsibilities for the public access facility at all times.**

(3) **The cognizant COTP may withdraw the exemption for a public access facility at any time the owner or operator fails to comply with any requirement of the COTP as a condition of the exemption or any measure ordered by the COTP pursuant to existing COTP authority.**

(e) **An owner or operator of a facility is not subject to this part if the facility receives only vessels to be laid-up, dismantled, or otherwise placed out of commission provided that the vessels are not carrying and do not receive cargo or passengers at that facility.**

§ 105.115 Compliance dates.

(a) **On or before December 31, 2003, facility owners or operators must submit to the cognizant COTP for each 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 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 facility owner or operator must be operating in compliance with this part.

§ 105.120 Compliance documentation.

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

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

(b) The FSP submitted for approval and an acknowledgement letter from the COTP stating that the Coast Guard is currently reviewing the FSP submitted for approval, and that the facility may continue to operate so long as the facility remains in compliance with the submitted FSP; or

(c) For facilities operating under a Coast Guard-approved Alternative Security Program as provided in §105.140, a copy of the Alternative Security Program the 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 facility owner or operator, stating which

Alternative Security Program the facility is using and certifying that the facility is in full compliance with that program.

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.

§ 105.125 Noncompliance.

When a facility must temporarily deviate from the requirements of this part, the facility owner or operator must notify the cognizant COTP, and either suspend operations or request and receive permission from the COTP to continue operating.

§ 105.130 Waivers.

Any facility owner or operator may apply for a waiver of any requirement of this part that the facility owner or operator considers unnecessary in light of the nature or operating conditions of the facility, prior to operating. A request for a waiver must be submitted in writing with justification to the Commandant (G-MP) at 2100 Second St., SW., Washington, DC 20593. The Commandant (G-MP) may require the facility owner or operator to provide data for use in determining the validity of the requested waiver. The Commandant (G-MP) may grant, in writing, a waiver with or without conditions only if the waiver will not reduce the overall security of the facility, its employees, visiting vessels, or ports.

[USCG-2003-14732, 68 FR 39322, July 1, 2003; 68 FR 41916, July 16, 2003]

§ 105.135 Equivalentents.

For any measure required by this part, the facility owner or operator may propose an equivalent as provided in §101.130 of this subchapter.

§ 105.140 Alternative Security Program.

(a) A facility owner or operator may use an Alternative Security Program approved under §101.120 of this subchapter if:

- (1) The Alternative Security Program is appropriate to that facility;
- (2) The Alternative Security Program is implemented in its entirety.

(b) A facility owner or operator using an Alternative Security Program approved under §101.120 of this subchapter must complete and submit to the cognizant COTP a Facility Vulnerability and Security Measures Summary (Form CG-6025) in appendix A to part 105—Facility Vulnerability and Security (CG-6025).

§ 105.145 Maritime Security (MARSEC) Directive.

Each facility owner or operator subject to this part must comply with any instructions contained in a MARSEC Directive issued under §101.405 of this subchapter.

§ 105.150 Right to appeal.

Subpart B—Facility Security Requirements**§ 105.200 Owner or operator.**

(a) Each facility owner or operator must ensure that the facility operates in compliance with the requirements of this part.

(b) For each facility, the facility owner or operator must:

(1) Define the security organizational structure and provide each person exercising security duties and responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate, in writing, by name or by title, a Facility Security Officer (FSO) and identify how the officer 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 facility operates in compliance with the approved FSP;

(6) Ensure that adequate coordination of security issues takes place between the facility and vessels that call on it, including the execution of a Declaration of Security (DoS) as required by this part;

(7) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility for visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with vessel operators in advance of a vessel's arrival. In coordinating such leave, facility owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations. The text of these treaties can be found on the U.S. Department of State's website at <http://www.state.gov/s/l/24224.htm>;

(8) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level;

(9) Ensure security for unattended vessels moored at the facility;

(10) Ensure the report of all breaches of security and transportation security incidents to the National Response Center in accordance with part 101 of this chapter; and

(11) Ensure consistency between security requirements and safety requirements.

§ 105.205 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.

(2) The same person may serve as the FSO for more than one facility, provided the facilities are in the same COTP zone and are not more than 50 miles apart. If a person serves as the FSO for more than one facility, the name of each facility for which he or she is the FSO must be listed in the Facility Security Plan (FSP) of each facility for which or she is the FSO.

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

(b) *Qualifications.* (1) The FSO must have general knowledge, through training or equivalent job experience, in the following:

(i) Security organization of the facility;

(ii) General vessel and facility operations and conditions;

(iii) Vessel and facility security measures, including the meaning and the requirements of the different MARSEC Levels;

(iv) Emergency preparedness, response, and contingency planning;

(v) Security equipment and systems, and their operational limitations; and

(vi) Methods of conducting audits, inspections, control, and monitoring techniques.

(2) In addition to knowledge and training required in paragraph (b)(1) of this section, the FSO must have knowledge of and receive training in the following, as appropriate:

(i) Relevant international laws and codes, and recommendations;

(ii) Relevant government legislation and regulations;

(iii) Responsibilities and functions of local, State, and Federal law enforcement agencies;

(iv) **Security** assessment methodology;

(v) Methods of facility security surveys and inspections;

(vi) Instruction techniques for security training and education, including security measures and procedures;

(vii) Handling sensitive security information and security related communications;

(viii) Current security threats and patterns;

(ix) Recognizing and detecting dangerous substances and devices;

(x) Recognizing characteristics and behavioral patterns of persons who are likely to threaten security;

(xi) Techniques used to circumvent security measures;

(xii) Conducting physical searches and non-intrusive inspections;

(xiii) Conducting security drills and exercises, including exercises with vessels; and

(xiv) Assessing security drills and exercises.

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

(1) Ensure that the Facility Security Assessment (FSA) is conducted;

(2) Ensure the development and implementation of a FSP;

(3) Ensure that an annual audit is conducted, and if necessary **that** the FSA and FSP are updated;

(4) Ensure the FSP is exercised per §105.220 of this part;

(5) Ensure that regular security inspections of the facility are conducted;

- (6) Ensure the security awareness and vigilance of the facility personnel;
- (7) Ensure adequate training to personnel performing facility security duties;
- (8) Ensure that occurrences that threaten the security of the facility are recorded and reported to the owner or operator;
- (9) Ensure the maintenance of records required by this part;
- (10) Ensure the preparation and the submission of any reports as required by this part;
- (11) Ensure the execution of any required Declarations of Security with **Masters, Vessel Security Officers or their designated representatives**;
- (12) Ensure the coordination of security services in accordance with the approved FSP;
- (13) Ensure that security equipment is properly operated, tested, calibrated, and maintained;
- (14) Ensure the recording and reporting of attainment changes in MARSEC Levels to the owner or operator and the cognizant COTP;
- (15) When requested, ensure that the Vessel Security Officers receive assistance in confirming the identity of visitors and service providers seeking to board the vessel through the facility;
- (16) Ensure notification, as soon as possible, to law enforcement personnel and other emergency responders to permit a timely response to any transportation security incident;
- (17) Ensure that the FSP is submitted to the cognizant COTP for approval, as well as any plans to change the facility or facility infrastructure prior to amending the FSP; and
- (18) Ensure that all facility personnel are briefed of changes in security conditions at the facility.

§ 105.210 Facility personnel with security duties.

Facility personnel responsible for security duties must have knowledge, through training or equivalent job experience, in the following, as appropriate:

- (a) Knowledge of current 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) Techniques used to circumvent security measures;
- (e) Crowd management and control techniques;
- (f) Security related communications;
- (g) Knowledge of emergency procedures and contingency plans;
- (h) Operation of security equipment and systems;
- (i) Testing, calibration, and maintenance of security equipment and systems;
- (j) Inspection, control, and monitoring techniques;
- (k) Relevant provisions of the Facility Security Plan (FSP);

- (l) Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores; and

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

§ 105.215 Security training for all other facility personnel.

All other facility personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge of, through training or equivalent job experience, in 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 as they apply to them, 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) Techniques used to circumvent security measures.

§ 105.220 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 facility reports attainment to the cognizant COTP.

(b) *Drills.* (1) 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 facility, facility personnel changes, the type of vessel the facility is serving, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.

(3) If a vessel is moored at the facility on the date the facility has planned to conduct any drills, the facility cannot require the vessel or vessel personnel to be a part of or participate in the facility's scheduled drill.

(c) *Exercises.* (1) 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 or seminar;
 - (iii) Combined with other appropriate exercises;
- 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 with applicable facility and vessel security plans or comprehensive port exercises.

(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 security program and must include substantial and active participation of FSOs, and may include government authorities and vessels visiting the facility. Requests for participation of Company and Vessel Security Officers in joint exercises should consider the security and work implications for the vessel.

§ 105.225 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 deletion, destruction, or amendment. The following records must be kept:

(1) *Training*. For **training under § 105.210**, 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, description of drill or exercise, list of participants, and any best practices or lessons learned which may improve the Facility Security Plan (FSP);

(3) *Incidents and breaches of security*. For each incident or breach of security, the date and time of occurrence, location within the facility, description of incident or breaches, to whom it was reported, and description of the response;

(4) *Changes in MARSEC Levels*. For each change in MARSEC Level, the date and time of notification received, and 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*. 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

(8) *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, 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.

§ 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; and

(3) Control access to the facility.

(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. Each location allowing means of access to the facility must be addressed;

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

(3) The means of identification required to allow access to the facility and for individuals and vehicles to remain on the facility without challenge; and

(4) The identification of 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 an identification system is established for checking the identification of facility personnel or other persons seeking access to the facility that:

(1) Allows identification of authorized and unauthorized persons at any MARSEC Level;

(2) Is coordinated, when practicable, with identification systems of vessels **or other transportation conveyances** that use the facility;

(3) Is updated regularly;

(4) Uses disciplinary measures to discourage abuse;

(5) Allows temporary or continuing access for facility personnel and visitors, including seafarers' chaplains and union representatives, through the use of a badge or other system to verify their identity; and

(6) Allows certain long-term, frequent vendor representatives to be treated more as employees than as visitors.

(d) The 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.

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

(1) Screen persons, baggage (including carry-on items), personal effects, and vehicles, for dangerous substances and devices at the rate specified in the approved FSP, **excluding government-owned vehicles on official business when government personnel present identification credentials for entry**;

(2) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Entering the 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 enter;

(3) Check the identification of any person seeking to enter the facility, including vessel passengers and crew, facility employees, vendors, personnel duly authorized by the cognizant authority, and visitors. This check includes confirming the reason for entry by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system required in paragraph (c) of this section;

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

(5) Designate restricted areas and provide appropriate access controls for these areas;

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

(7) Deter unauthorized access to the facility and to designated restricted areas within the facility;

(8) Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel; and

(9) Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between the facility and a vessel.

(f) *MARSEC Level 2*. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the 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) Increasing the frequency and detail of the screening of persons, baggage, and personal effects for dangerous substances and devices entering the facility;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to guard access points and patrol the perimeter of the facility to deter unauthorized access;

(4) Limiting the number of access points to the facility by closing and securing some access points and providing physical barriers to impede movement through the remaining access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the facility, which may include, using waterborne patrols to enhance security around the facility; or

(7) **Except for government-owned vehicles on official business when government personnel present identification credentials for entry, screening** vehicles and their contents for dangerous substances and devices at the rate specified for MARSEC Level 2 in the approved FSP.

(g) *MARSEC Level 3*. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the 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) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied baggage more extensively; for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage;

(3) Being prepared to cooperate with responders and facilities;

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

(5) Suspending access to the facility;

(6) Suspending cargo operations;

(7) Evacuating the facility;

(8) Restricting pedestrian or vehicular movement on the grounds of the facility; or

(9) Increasing security patrols within the facility.

§ 105.260 Security measures for restricted areas.

(a) *General*. The 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 facility;

(3) Protect the facility;

(4) Protect vessels using and serving the facility;

(5) Protect sensitive security areas within the facility;

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

(7) Protect cargo and vessel stores from tampering.

(b) *Designation of Restricted Areas.* The facility owner or operator must ensure restricted areas are designated within the 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 facility owner or operator may also designate the entire facility as a restricted area. Restricted areas must include, as appropriate:

(1) Shore areas immediately adjacent to each vessel moored at the facility;

(2) Areas containing sensitive security information, including cargo documentation;

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

(4) Areas containing critical facility infrastructure, including:

(i) Water supplies;

(ii) Telecommunications;

(iii) Electrical system; and

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

(5) Manufacturing or processing areas and control rooms;

(6) Locations in the facility where access by vehicles and personnel should be restricted;

(7) Areas designated for loading, unloading or storage of cargo and stores; and

(8) Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes.

(c) The owner or operator must ensure that all restricted areas have clearly established security measures to:

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

(2) Determine which persons other than 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;

(5) Define the times when access restrictions apply;

(6) Clearly mark all restricted areas and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security;

(7) Control the entry, parking, loading and unloading of vehicles;

(8) Control the movement and storage of cargo and vessel stores; and

(9) Control unaccompanied baggage or personal effects.

(d) *MARSEC Level 1.* At MARSEC Level 1, the 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) Assigning personnel to control access to restricted areas;

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

(5) Patrolling or monitoring the perimeter of restricted areas;

(6) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry or movement within restricted areas;

(7) Directing the parking, loading, and unloading of vehicles within a restricted area;

(8) Controlling unaccompanied baggage and or personal effects after screening;

(9) Designating restricted areas for performing inspections of cargo and vessel stores while awaiting loading; and

(10) Designating temporary restricted areas to accommodate facility operations. If temporary restricted areas are designated, the FSP must include a requirement to conduct a security sweep of the designated temporary restricted area 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 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) Increasing the intensity and frequency of monitoring and access controls on existing restricted access areas;

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

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

(4) Restricting parking adjacent to vessels;

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

(6) Using continuously monitored and recorded surveillance equipment;

(7) Enhancing the number and frequency of patrols, including waterborne patrols undertaken on the boundaries of the restricted areas and within the areas; or

(8) Establishing and 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 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 facility.

§ 105.265 Security measures for handling cargo.

(a) *General.* The facility owner or operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the vessel, are implemented in order to:

- (1) Deter tampering;
- (2) Prevent cargo that is not meant for carriage from being accepted and stored at the facility **without the knowing consent of the facility owner or operator**;
- (3) Identify cargo that is approved for loading onto vessels interfacing with the facility;
- (4) Include cargo control procedures at access points to the facility;
- (5) Identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up;
- (6) Restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate;
- (7) Ensure the release of cargo only to the carrier specified in the cargo documentation;
- (8) **When there are regular or repeated cargo operations with the same shipper, coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedure; and**
- (9) **Create, update, and maintain a continuous inventory of all dangerous goods and hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods and hazardous substances.**

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

- (1) **Unless unsafe to do so, routinely** check cargo, cargo transport units, and cargo storage areas within the facility prior to, and during, cargo handling operations **for evidence of tampering**;
- (2) Check that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation;
- (3) Screen vehicles; and
- (4) Check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the 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) Conducting check of cargo, containers or other cargo transport units, and cargo storage areas within the facility for **evidence of tampering**;

(2) Intensifying checks, as appropriate, to ensure that only the documented cargo enters the facility, is temporarily stored there, and then loaded onto the vessel;

(3) Intensifying the screening of vehicles;

(4) Increasing frequency and detail in checking of seals and other methods used to prevent tampering;

(5) **Coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures**;

(6) Increasing the frequency and intensity of visual and physical inspections; or

(7) Limiting the number of locations where dangerous goods and hazardous substances, including certain dangerous cargoes, can be stored.

(d) *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 the approved FSP. These additional security measures may include:

(1) Restricting or suspending cargo movements or operations within all or part of the facility or specific vessels;

(2) Being prepared to cooperate with responders and vessels; or

(3) Verifying the inventory and location of any dangerous goods and hazardous substances, including certain dangerous cargoes, held within the facility and their location.

§ 105.270 Security measures for delivery of vessel stores and bunkers.

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

(1) Check vessel stores for package integrity;

(2) Prevent vessel stores from being accepted without inspection;

(3) Deter tampering;

(4) For vessels that routinely use a facility, establish and execute standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation; and

(5) Check vessel stores by the following means:

(i) Visual examination;

(ii) Physical examination;

(iii) Detection devices, such as scanners; or

(iv) Canines.

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

(1) Screen vessel stores at the rate specified in the approved Facility Security Plan (FSP);

(2) Require advance notification of vessel stores or bunkers delivery, including a list of stores, delivery vehicle driver information, and vehicle registration information;

(3) Screen delivery vehicles at the frequencies specified in the approved FSP; and

(4) Escort delivery vehicles within the facility at the rate specified by the approved FSP.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the 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) Detailed screening of vessel stores;

(2) Detailed screening of all delivery vehicles;

(3) Coordinating with vessel personnel to check the order against the delivery note prior to entry to the facility;

(4) Ensuring delivery vehicles are escorted within the facility; or

(5) Restricting or prohibiting the entry of vessel stores that will not leave the facility within a specified period.

(d) *MARSEC Level 3.* In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner and operator must ensure implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. Examples of these additional security measures may include:

(1) Checking all vessel stores more extensively;

(2) Restricting or suspending delivery of vessel stores; or

(3) Refusing to accept vessel stores on the facility.

§ 105.275 Security measures for monitoring.

(a) *General.* The 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, security guards, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment, as specified in the approved Facility Security Plan (FSP), the:

(1) Facility and its approaches, on land and water;

(2) Restricted areas within the facility; and

(3) Vessels at the facility and areas surrounding the vessels.

(b) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the security measures in this section are implemented at all times, including the period from sunset to sunrise and periods of limited visibility. For each facility, ensure monitoring capability that:

(1) When automatic intrusion-detection devices are used, activates an audible or visual alarm, or both, at a location that is continuously attended or monitored;

(2) Is able to function continually, including consideration of the possible effects of weather or of a power disruption;

(3) Monitors the facility area, including shore and waterside access to it;

(4) Monitors access points, barriers and restricted areas;

(5) Monitors access and movements adjacent to vessels using the facility, including augmentation of lighting provided by the vessel itself; and

(6) Limits lighting effects, such as glare, and their impact on safety, navigation, and other security activities.

(c) *MARSEC Level 2.* In addition to the security measures for MARSEC Level 1 in this section, at MARSEC Level 2, the 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 measures may include:

(1) Increasing the coverage and intensity of surveillance equipment, including the provision of additional surveillance coverage;

(2) Increasing the frequency of foot, vehicle or waterborne patrols;

(3) Assigning additional security personnel to monitor and patrol; or

(4) Increasing the coverage and intensity of lighting, including the provision of additional lighting and coverage.

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

(1) Switching on all lighting within, or illuminating the vicinity of, the facility;

(2) Switching on all surveillance equipment capable of recording activities within or adjacent to the facility;

(3) Maximizing the length of time such surveillance equipment can continue to record; or

(4) Complying with the instructions issued by those responding to the security incident.

§ 105.280 Security incident procedures.

For each MARSEC Level, the facility owner or operator must ensure the Facility Security Officer and facility security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical facility and vessel-to-facility interface operations;

(b) Evacuate the facility in case of security threats or breaches of security;

(c) Report security incidents as required in §101.305 of this subchapter;

(d) Brief all facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

(e) Secure non-critical operations in order to focus response on critical operations.

§ 105.285 Additional requirements-passenger and ferry facilities.

(a) **At all MARSEC Levels**, the owner or operator of a passenger or ferry facility must ensure, in coordination with a vessel moored at the facility, that the following security measures are implemented in addition to the requirements of this part:

(1) **Establish** separate areas to segregate unchecked persons and personal effects from checked persons and personal effects;

(2) Ensure that a defined percentage of vehicles to be loaded aboard are screened prior to loading, in accordance with a MARSEC Directive or other orders issued by the Coast Guard;

(3) Ensure that all unaccompanied vehicles to be loaded on passenger vessels are screened prior to loading;

(4) Deny passenger access to restricted areas unless supervised by facility security personnel; and

(5) In a facility with a public access area designated under §105.106, provide sufficient security personnel to monitor all persons within the area.

(b) At MARSEC Level 2, in addition to the requirements in paragraph (a) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under § 105.106 must increase the intensity of monitoring of the public access area.

(c) At MARSEC Level 3, in addition to the requirements in paragraph (a) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under § 105.106 must increase the intensity of monitoring and assign additional security personnel to monitor the public access area.

§ 105.290 Additional requirements-cruise ship terminals.

At all MARSEC Levels, in coordination with a vessel moored at the facility, the facility owner or operator must ensure the following security measures:

(a) Screen all persons, baggage, and personal effects for dangerous substances and devices;

(b) Check the identification of all persons seeking to board the vessel. This includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, government identification or visitor badges, or work orders;

(c) Designate holding, waiting, or embarkation areas to segregate screened persons and their personal effects awaiting embarkation from unscreened persons and their personal effects;

(d) Provide additional security personnel to designated holding, waiting, or embarkation areas; and

(e) Deny passenger access to restricted areas unless supervised by facility security personnel.

§ 105.295 Additional requirements-Certain Dangerous Cargo (CDC) facilities.

(a) At all MARSEC Levels, owners or operators of CDC facilities must ensure the implementation of the following security measures in addition to the requirements of this part:

(1) Escort all visitors, contractors, vendors, and other non-facility employees at all times while on the facility, if access identification is not provided. Escort provisions do not apply to prearranged cargo deliveries;

(2) Control the parking, loading, and unloading of vehicles within a facility;

(3) Require security personnel to record or report their presence at key points during their patrols;

(4) Search unmanned or unmonitored waterfront areas for dangerous substances and devices prior to a vessel's arrival at the facility; and

(5) Provide an alternate or independent power source for security and communications systems.

(b) At MARSEC Level 2, in addition to the requirements for MARSEC Level 1, owners or operators of CDC facilities must ensure the implementation of the following security measures:

(1) Release cargo only in the presence of the Facility Security Officer (FSO) or a designated representative of the FSO; and

(2) Continuously patrol restricted areas.

(c) At MARSEC Level 3, in addition to the requirements for MARSEC Level 1 and MARSEC Level 2, owners or operators of CDC facilities must ensure the facilities are continuously guarded and restricted areas are patrolled.

§ 105.296 Additional requirements-barge fleeting facilities.

(a) At MARSEC Level 1, in addition to the requirements of this part, an owner or operator of a barge fleeting facility must ensure the implementation of the following security measures:

(1) Designate one or more restricted areas within the barge fleeting facility to handle those barges carrying, in bulk, cargoes regulated by 46 CFR chapter I, subchapters D or O, or Certain Dangerous Cargoes;

(2) Maintain a current list of vessels and cargoes in the designated restricted area; and

(3) Ensure that at least one towing vessel is available to service the fleeting facility for every 100 barges within the facility.

(b) At MARSEC Level 2, in addition to the requirements of this part and MARSEC Level 1 requirements, an owner or operator of a barge fleeting facility must ensure security personnel are assigned to monitor or patrol the designated restricted area within the barge fleeting facility.

(c) At MARSEC Level 3, in addition to the requirements of this part and MARSEC Level 2 requirements, an owner or operator of a barge fleeting facility must ensure that both land and waterside perimeters of the designated restricted area within the

barge fleeting facility are continuously monitored or patrolled.

Subpart C—Facility Security Assessment (FSA)

§ 105.300 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 common FSA may be conducted for more than one similar facility provided the FSA reflects any facility-specific characteristics that are unique.

(c) Third parties may be used in any aspect of the FSA if they have the appropriate skills and if the Facility Security Officer (FSO) 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 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) Techniques used to circumvent security measures;
- (5) Methods used to cause a security incident;
- (6) Effects of dangerous substances and devices on structures and facility services;
- (7) Facility security requirements;
- (8) 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) Facility and vessel operations.

§ 105.305 Facility Security Assessment (FSA) requirements.

(a) *Background.* The 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 facility, including:
 - (i) The location of each active and inactive access point to the facility;
 - (ii) The number, reliability, and security duties of 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 maintenance equipment, cargo spaces, storage areas, and unaccompanied baggage storage;
 - (vii) Location of escape and evacuation routes and assembly stations; and

(viii) Existing security and safety equipment for protection of personnel and visitors;

(2) Response procedures for fire or other emergency conditions;

(3) Procedures for monitoring facility and vessel personnel, vendors, repair technicians, and dock workers;

(4) Existing contracts with private security companies and existing agreements with local or municipal agencies;

(5) Procedures for controlling keys and other access prevention systems;

(6) Procedures for cargo and vessel stores operations;

(7) Response capability to security incidents;

(8) Threat assessments, including the purpose and methodology of the assessment, for the port in which the facility is located or at which passengers embark or disembark;

(9) Previous reports on security needs; and

(10) Any other existing security procedures and systems, equipment, communications, and facility personnel.

(b) *On-scene survey.* The facility owner or operator must ensure that an on-scene survey of each facility is conducted. The on-scene survey examines and evaluates existing 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 facility owner or operator must ensure that the FSO analyzes the 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) Waterside and shore-side access to the facility and vessel berthing at the facility;

(ii) Structural integrity of the piers, facilities, and associated structures;

(iii) Existing security measures and procedures, including identification systems;

(iv) Existing security measures and procedures relating to services and utilities;

(v) Measures to protect radio and telecommunication equipment, including computer systems and networks;

(vi) Adjacent areas that may be exploited during or for an attack;

(vii) Areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the facility;

(viii) Existing agreements with private security companies providing waterside and shore-side security services;

(ix) Any conflicting policies between safety and security measures and procedures;

(x) Any conflicting facility operations and security duty assignments;

(xi) Any enforcement and personnel constraints;
 (xii) Any deficiencies identified during daily operations or training and drills; and

(xiii) 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 facility or of a vessel moored at the facility;

(ii) Hijacking or seizure of a vessel moored at the facility or of persons on board;

(iii) Tampering with cargo, essential equipment or systems, or stores of a vessel moored at the facility;

(iv) Unauthorized access or use including the presence of stowaways;

(v) Smuggling dangerous substances and devices to the facility;

(vi) Use of a vessel moored at the facility to carry those intending to cause a security incident and their equipment;

(vii) Use of a vessel moored at the facility as a weapon or as a means to cause damage or destruction;

(viii) **Impact on the facility and its operations due to a blockage** of entrances, locks, and approaches; and

(ix) **Use of the facility as a transfer point for nuclear, biological, radiological, explosive, or chemical weapons;**

(3) Threat assessments by Government agencies;

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

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

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

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

(d) *FSA report.* (1) The facility owner or operator must ensure that a written FSA report is prepared and included as 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 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 facility.

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

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

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

(vi) Relevant transportation infrastructure; and

(vii) Utilities.

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

(i) **Facility personnel;**

(ii) **Passengers, visitors, vendors, repair technicians, vessel personnel, etc.;**

(iii) **Capacity to maintain emergency response;**

(iv) **Cargo, particularly dangerous goods and hazardous substances;**

(v) **Delivery of vessel stores;**

(vi) **Any facility security communication and surveillance systems; and**

(vii) **Any other facility 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 duties and security assignments;**

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

(i) **Ensuring performance of all security duties;**

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

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

(iv) **Procedures for the handling of cargo and the delivery of vessel stores;**

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

(vi) **Monitoring the facility and areas adjacent to the pier; 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.**

§ 105.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan required in **§ 105.410 of this part**.

(b) A facility owner or operator may generate and submit a report that contains the Facility Security Assessment for more than one facility subject to this part, to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP.

(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.

Subpart D—Facility Security Plan (FSP)**§ 105.400 General.**

(a) The Facility Security Officer (FSO) must ensure a Facility Security Plan (FSP) is developed and implemented for each facility for which he or she is designated as FSO. The FSP:

- (1) Must identify the FSO by name and 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 facility to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP.

(b) The FSP must be submitted for approval to the cognizant COTP in a written or electronic format. **Information** for submitting the FSP electronically can be found at <http://www.uscg.mil/HQ/MSC>.

(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.

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

(a) A 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 the list, the facility owner or operator must ensure that the FSP contains an index identifying the location of each of the following sections:

- (1) Security administration and organization of the 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, including designated public access areas;

(11) Security measures for restricted areas;

(12) Security measures for handling cargo;

(13) Security measures for delivery of vessel stores and bunkers;

(14) Security measures for monitoring;

(15) Security incident procedures;

(16) Audits and security plan amendments;

(17) Facility Security Assessment (FSA) report; and

(18) Facility Vulnerability and Security Measures Summary (Form CG-6025) in appendix A to part 105—Facility Vulnerability and Security Measures Summary (CG-6025).

(b) The facility owner or operator must ensure that the FSP describes in detail how each of the individual requirements of subpart B of this part will be met.

(c) The Facility Vulnerability and Security Measures Summary (Form CG-6025) must be completed using information in the FSA concerning identified vulnerabilities and information in the FSP concerning security measures in mitigation of these vulnerabilities.

§ 105.410 Submission and approval.

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

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

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

(b) Owners or operators of 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 COTP 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 facility where they share similarities in design and operations, if authorized and approved by each cognizant COTP.

(e) Each facility owner or operator that submits one FSP to cover two or more facilities of similar design and operation must address facility-specific information that includes the design and operational characteristics of each facility and must complete a separate Facility Vulnerability and Security Measures Summary (Form CG-6025), in appendix A to part 105—Facility Vulnerability and Security Measures Summary (CG-6025), for each facility covered by the plan.

(f) A FSP that is approved by the cognizant COTP is valid for five years from the date of its approval.

§ 105.415 Amendment and audit.

(a) *Amendments.* (1) Amendments to a ~~FSP~~ **Facility Security Plan (FSP)** that is approved by the cognizant COTP may be initiated by:

(i) The facility owner or operator; or

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

(2) Proposed amendments must be submitted to the cognizant COTP. If initiated by the facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant COTP allows a shorter period. The cognizant COTP will approve or disapprove the proposed amendment in accordance with § 105.410 of this subpart.

(3) **Nothing in this section should be construed as limiting the 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 COTP 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 there is a change in the owner or operator, the Facility Security Officer (FSO) must amend the FSP to include the name and contact information of the new facility owner or operator and submit the affected portion of the FSP for review and approval in accordance with § 105.410 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) The FSP must be audited if there is a change in the facility's ownership or operator, or if there have been modifications to the facility, 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 facility may be limited to those sections of the FSP affected by the facility modifications.

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

(i) Have knowledge of methods for conducting audits and inspections, and security, 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 amendment of either the FSA or FSP, the FSO must submit, in accordance with § 105.410 of this subpart, the amendments to the cognizant COTP 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.

Appendix A to Part 105—Facility Vulnerability and Security Measures Summary (Form CG-6025).

| | | | | | |
|---|--|--|--|--|--|
| U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-6025 (05/03) | | FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY | | OMB APPROVAL NO. 1625-0077 | |
| An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 60 minutes. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: Commandant (G-MP), U.S. Coast Guard, 2100 2nd St. SW, Washington D.C. 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0077), Washington, DC 20503. | | | | | |
| FACILITY IDENTIFICATION | | | | | |
| 1. Name of Facility | | | | | |
| 2. Address of Facility | | | 3. Latitude | | |
| | | | 4. Longitude | | |
| | | | 5. Captain of the Port Zone | | |
| 6. Type of Operation (check all that apply) | | | | | |
| <input type="checkbox"/> Break Bulk <input type="checkbox"/> Dry Bulk <input type="checkbox"/> Container <input type="checkbox"/> RO-RO | | <input type="checkbox"/> Petroleum <input type="checkbox"/> Chemical <input type="checkbox"/> LHG/LNG <input type="checkbox"/> Explosives and other dangerous cargo | | <input type="checkbox"/> Certain Dangerous Cargo <input type="checkbox"/> Barge Fleetings <input type="checkbox"/> Offshore Support <input type="checkbox"/> Passengers (Subchapter H) <input type="checkbox"/> Passengers (Ferries) <input type="checkbox"/> Passengers (Subchapter K) <input type="checkbox"/> Military Supply | |
| | | | | <input type="checkbox"/> If other, explain: <div style="border: 1px solid black; height: 20px; width: 100%;"></div> | |
| VULNERABILITY AND SECURITY MEASURES | | | | | |
| 7a. Vulnerability | | | 7b. Vulnerability Category | | |
| | | | <input type="checkbox"/> If other, explain | | |
| 8a. Selected Security Measures (MARSEC Level 1) | | | 8b. Security Measures Category | | |
| | | | <input type="checkbox"/> If other, explain | | |
| 9a. Selected Security Measures (MARSEC Level 2) | | | 9b. Security Measures Category | | |
| | | | <input type="checkbox"/> If other, explain | | |
| 10a. Selected Security Measures (MARSEC Level 3) | | | 10b. Security Measures Category | | |
| | | | <input type="checkbox"/> If other, explain | | |
| VULNERABILITY AND SECURITY MEASURES | | | | | |
| 7a. Vulnerability | | | 7b. Vulnerability Category | | |
| | | | <input type="checkbox"/> If other, explain | | |
| 8a. Selected Security Measures (MARSEC Level 1) | | | 8b. Security Measures Category | | |
| | | | <input type="checkbox"/> If other, explain | | |
| 9a. Selected Security Measures (MARSEC Level 2) | | | 9b. Security Measures Category | | |
| | | | <input type="checkbox"/> If other, explain | | |
| 10a. Selected Security Measures (MARSEC Level 3) | | | 10b. Security Measures Category | | |
| | | | <input type="checkbox"/> If other, explain | | |

| | | |
|--|---|-------------------------------|
| U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-6025A (05/03) | VULNERABILITY AND SECURITY MEASURES ADDENDUM | OMB APPROVAL NO. 1625-0077 |
| An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 60 minutes. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: Commandant (G-MP), U.S. Coast Guard, 2100 2nd St. SW, Washington D.C. 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0077), Washington, DC 20503. This form may only be used in addition to form CG-6025, never alone. | | |
| NAME OF FACILITY (Use same Name as Block 1., of CG-6025) | | |
| 7a. Vulnerability | 7b. Vulnerability Category | |
| | <input type="checkbox"/> If other, explain | |
| 8a. Selected Security Measures (MARSEC Level 1) | 8b. Security Measures Category | |
| | <input type="checkbox"/> If other, explain | |
| 9a. Selected Security Measures (MARSEC Level 2) | 9b. Security Measures Category | |
| | <input type="checkbox"/> If other, explain | |
| 10a. Selected Security Measures (MARSEC Level 3) | 10b. Security Measures Category | |
| | <input type="checkbox"/> If other, explain | |
| 7a. Vulnerability | 7b. Vulnerability Category | |
| | <input type="checkbox"/> If other, explain | |
| 8a. Selected Security Measures (MARSEC Level 1) | 8b. Security Measures Category | |
| | <input type="checkbox"/> If other, explain | |
| 9a. Selected Security Measures (MARSEC Level 2) | 9b. Security Measures Category | |
| | <input type="checkbox"/> If other, explain | |
| 10a. Selected Security Measures (MARSEC Level 3) | 10b. Security Measures Category | |
| | <input type="checkbox"/> If other, explain | |
| 7a. Vulnerability | 7b. Vulnerability Category | |
| | <input type="checkbox"/> If other, explain | |
| 8a. Selected Security Measures (MARSEC Level 1) | 8b. Security Measures Category | |
| | <input type="checkbox"/> If other, explain | |
| 9a. Selected Security Measures (MARSEC Level 2) | 9b. Security Measures Category | |
| | <input type="checkbox"/> If other, explain | |
| 10a. Selected Security Measures (MARSEC Level 3) | 10b. Security Measures Category | |
| | <input type="checkbox"/> If other, explain | |

INSTRUCTIONS FOR THE CG-6025
FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY

This form satisfies the requirements for Facility Vulnerability and Security Measures Summary submission found in the Code of Federal Regulations for Facility Security. Form CG-6025A, Vulnerability and Security Measures Addendum, may be used as a continuation of form CG-6025, in order to submit additional vulnerabilities and security measures. If a facility owner or operator submits a Facility Vulnerability and Security Measures Summary pertaining to more than one facility, form CG-6025, shall be submitted to document each additional facility.

| | | | |
|----------|--|-----------|---|
| BLOCK 1 | Self-Explanatory. | BLOCK 8b | Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided. |
| BLOCK 2 | Street Address. | | |
| BLOCK 3 | If available, provide latitude to nearest tenth of a minute. | | |
| BLOCK 4 | If available, provide longitude to nearest tenth of a minute. | BLOCK 9a | Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 2 that will mitigate the vulnerability you addressed. |
| BLOCK 5 | Provide the Captain of the Port Zone from the list below in which your facility resides. Their respective zones are described in 33 CFR Part 3. | BLOCK 9b | Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided. |
| BLOCK 6 | Check all applicable operations that are conducted at your facility. If you select other, please explain in the box provided. | | |
| BLOCK 7a | Enter a concise description of a vulnerability identified in your facility's assessment. Provide location information if appropriate. | BLOCK 10a | Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 3 that will mitigate the vulnerability you addressed. |
| BLOCK 7b | Enter the vulnerability identification code from the KEY to categorically identify the vulnerability you described. More than one category may be used. If you select other, please explain in the box provided. | BLOCK 10b | Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided. |
| BLOCK 8a | Enter a concise description of a selected security measure identified in the plan for MARSEC Level 1 that will mitigate the vulnerability you addressed. | | |

CAPTAIN OF THE PORT ZONE:

| | | | |
|----------------|------------------------|--------------|------------------|
| Anchorage | Honolulu | Mobile | Puget Sound |
| Baltimore | Houston-Galveston | Morgan City | San Diego |
| Boston | Huntington | New Orleans | San Francisco |
| Buffalo | Jacksonville | New York | San Juan |
| Charleston | Juneau | Paducah | Sault Ste. Marie |
| Chicago | Long Island Sound | Philadelphia | Savannah |
| Cleveland | Los Angeles/Long Beach | Pittsburgh | St. Louis |
| Corpus Christi | Louisville | Port Arthur | Tampa |
| Detroit | Memphis | Portland, ME | Toledo |
| Duluth | Miami | Portland, OR | Valdez |
| Guam | Milwaukee | Providence | Wilmington |
| Hampton Roads | | | |

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 | | |
