

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;

## Coast Guard, DHS

## § 105.400

(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.

[USCG-2003-14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003]

### § 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.

[USCG-2003-14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003]

## 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.