

personnel, as well as actions for securing vessels moored to the facility and evacuating passengers and crew.

Declaration of Security (DoS)

A Declaration of Security is a written agreement between the facility and a vessel that provides a means for ensuring that critical security concerns are properly addressed prior to and during a vessel-to-facility interface. The Declaration of Security addresses security by delineating responsibilities for security arrangements and procedures between a vessel and facility. This requirement is similar to the existing U.S. practice for vessel-to-facility oil transfer proceedings.

Only certain passenger vessels and vessels carrying Certain Dangerous Cargoes, in bulk, will complete a Declaration of Security for every evolution regardless of the MARSEC Level. At MARSEC Levels 2 and 3, all vessels and facilities would need to complete the Declaration of Security.

Facilities that frequently receive the same vessel may execute a continuing Declaration of Security—a single Declaration of Security for multiple visits.

All Declarations of Security must state the security activities for which the facility and vessel are responsible during vessel-to-facility interfaces. Declarations of Security must be kept as part of the facility's recordkeeping.

Facility Security Assessment (FSA)

This rule requires all regulated facilities to complete a Facility Security Assessment, which is an essential and integral part of the process of developing and updating the required Facility Security Plan. The Facility Security Plan is based on the results of the Facility Security Assessment. The Facility Security Officer must examine and evaluate existing facility protective measures, procedures, and operations.

The Facility Security Officer must also examine each identified point of access, including rail access, roads, waterside, and gates, and evaluate its potential for use by individuals who might engage in unlawful acts, including individuals with legitimate access, as well as those seeking unauthorized entry.

Each facility owner or operator is required to document and retain its Facility Security Assessment for a period of five years. Prior to conducting a Facility Security Assessment, the Facility Security Officer is responsible for researching and using available information on the assessment of threat for the port at which the facility is located, as well as vessels that would

call on the facility. The first step in the facility security process is to conduct an on-scene survey. The on-scene survey is used to examine and evaluate existing facility protective measures, procedures and operations. In conducting the Facility Security Assessment, the facility owner or operator must ensure that the Facility Security Officer analyzes the facility background information and the results of the on scene survey, and considering the requirements of this interim rule, provide recommendation to establish and prioritize the security measures that should be included in the Facility Security Plan. The facility owner or operator then must ensure that a written Facility Security Assessment report is prepared and included in the Facility Security Plan. The Facility Security Assessment must be reviewed and updated each time the Facility Security Plan is revised and when the Facility Security Plan is submitted for re-approval every five years. The facility owner or operator then must ensure that a written Facility Security Assessment report is prepared and included as an appendix to the Facility Security Plan.

The Facility Security Officer is also responsible for ensuring that the Facility Security Assessment is periodically reviewed and updated, taking into account changes in the facility and its operations. Before a plan could be renewed or revised, a new Facility Security Assessment would need to be conducted.

The Facility Security Officer is responsible for obtaining and recording any specific information required to conduct the Facility Security Assessment.

Facility Security Plan (FSP)

This subpart contains requirements for Facility Security Plans. The requirements discussed in this subpart are consistent with requirements in the ISPS Code.

Facility Security Plans must incorporate the results of the required Facility Security Assessment and consider the recommended measures appropriate to each facility.

Facility Security Plans can be combined with or complement existing safety management systems. The plans may be kept in an electronic format, protected by means to prevent it from being deleted, destroyed or overwritten. The plans must also be protected from unauthorized access or disclosure.

Facility Security Plans required under this rulemaking must contain:

- A list of measures and equipment needed to prevent or deter dangerous substances and devices which could be

used against people, vessels or ports and the carriage of which is not authorized from being introduced by any means on to the facility;

- Requirements for the prevention of unauthorized access to the facility and to restricted areas of the facility;

- Documented procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the facility or the vessel-to-port interface;

- Documented procedures for evacuation in case of security threats or breaches of security;

- Procedures for training, exercises, and drills associated with the plan;

- Documented procedures for interfacing with port and vessel security activities;

- Documented procedures for the periodic review of the Facility Security Plan and for updating it;

- Documented procedures for reporting security incidents;

- Written designation of the Facility Security Officer;

- A list of the duties and responsibilities of all facility personnel with a security role;

- A list of measures to ensure the security of information contained in the plan;

- A maintenance system to maintain operational readiness of all required equipment using manufacturers' recommended maintenance instructions and periodic inspection;

- A list of measures needed to ensure effective security of cargo, cargo processing, and the cargo-handling equipment at the facility; and

- A completed Facility Vulnerability and Security Measures Summary (Form CG-6025) for each facility covered by the Plan.

Submission and Approval of Security Plan

The Facility Security Plan, including the Facility Security Assessment report and the Facility Vulnerability and Security Measures Summary (Form CG-6025), must be submitted to and reviewed by the cognizant COTP. Once the COTP finds that the plan meets the security requirements in part 105, the submitter will receive an approval letter that may contain conditions of the approval.

If the cognizant COTP requires more time than is indicated in the requirements of the interim rule to review a submitted Facility Security Plan, the cognizant COTP may return to the submitter a written acknowledgement stating that the Coast Guard is currently reviewing the