

- Security measures for restricted areas;
- Security measures for handling cargo;
- Security measures for delivery of vessel stores and bunkers; and
- Security measures for monitoring.

Security Incident Procedures

Each vessel owner or operator must develop security incident procedures for responding to transportation security incidents. The security incident procedures must explain the vessel's reaction to an emergency, including the notification and coordination with local, State, and federal authorities and Under Secretary of Emergency Preparedness and Response. The security incident procedures must also explain actions for securing the vessel and evacuating passengers and crew.

Declaration of Security (DoS)

A Declaration of Security 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 a 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 will complete a Declaration of Security for every evolution regardless of the Maritime Security Level. At Maritime Security Levels 2 and 3, all vessels and facilities would need to complete the Declaration of Security.

Vessels that frequently call on the same facility 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-vessel or vessel-to-facility interfaces. Declarations of Security must be kept as part of the vessel's recordkeeping.

Vessels that are operating at a higher Security Level than the port that the vessel is calling at may request a Declaration of Security with the facility, and the facility must complete a Declaration of Security with the vessel. Additionally, a facility may request that a vessel complete a Declaration of Security with the facility as appropriate for that facility's Security Plan or direction of the COTP. If the facility owner or operator requires a Declaration of Security, the vessel must comply. The conditions under which a vessel may

request a Declaration of Security from the facility must be included in the Vessel Security Plan.

Vessel Security Assessment (VSA)

This interim rule requires all vessels covered by part 104 to conduct a Vessel Security Assessment, which is an essential and integral part of the process for developing and updating the required Vessel Security Plan. The Vessel Security Assessment is based in part on an on-scene security survey, which details the overall assessment of the vessel including any existing security measures, and includes a written report documenting the vulnerabilities and mitigation strategies of the vessel. As discussed in the interim rule "Implementation of National Maritime Security Initiatives" (USCG-2003-14792), 33 CFR 101.510 lists the various assessment tools that may be used to meet the risk assessment requirements in parts 104 through 106 of this subchapter. The assessment tools listed are sufficient to enable the development of the Vessel Security Program. This list is also provided to ensure that the Vessel Security Assessment is consistent with other modal assessments. We are working with other agencies to develop assessment tools that are sensitive to the diversity of the National Marine Transportation System to ensure consistent levels of security throughout the entire System. The designated Company Security Officer must conduct the on-scene survey by examining and evaluating existing vessel protective measures, procedures, and operations. Using the information obtained in the on-scene survey, the Company Security Officer must ensure the completion of the Vessel Security Assessment. The Vessel Security Assessment identifies and evaluates, in writing, existing security measures; key vessel operations; the likelihood of possible threats to key vessel operations; and weaknesses, including human factors in the infrastructure, policies, and procedures of the vessel.

It also includes a written summary of how the assessment was conducted; each vulnerability found during the assessment; and countermeasures that could be used to address each vulnerability. The Vessel Security Assessment must be reviewed and updated each time the Vessel Security Plan is revised and when the Vessel Security Plan is submitted for re-approval every 5 years.

Vessel Security Plan (VSP)

This interim rule requires each vessel owner or operator to develop an

effective Vessel Security Plan that incorporates detailed preparedness, prevention, and response activities for each Maritime Security Level, along with the organizations or personnel responsible for carrying out those activities. The requirements discussed in this part are consistent with requirements in the ISPS Code.

The Vessel Security Plan is a document, written in English, that is prepared in response to the Vessel Security Assessment and approved by the Coast Guard. A single Vessel Security Plan can apply to more than one vessel to the extent that they share physical characteristics and operations.

In addition to other things, the Vessel Security Plan must: respond specifically to any recommendations made by the Vessel Security Assessment; describe how, at each Maritime Security Level, the vessel will apply the security measures required in these regulations; state the Master's authority; must detail the organizational structure of security for the vessel; detail the duties and responsibilities of all vessel and company personnel with a security role; detail the vessel's relationship with the Company, facilities, other vessels, and relevant authorities with security responsibility; provide regular audit of the Vessel Security Plan and its amendment in response to experience or changing circumstances; and establish the procedures needed to assess the continuing effectiveness of security procedures and all security related equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction.

The responsibility for barge security lies not only with the barge owner or operator but also with the towing vessel, fleeting facility, and facility where the barge is moored. Hence, security plans for vessels and facilities that interface with unmanned vessels (e.g. unmanned barges) must include additional provisions to address the risk of the unmanned vessels that they will receive or handle. Given the simple design of a typical barge and the wide range of products that may be transported within a single tow or moored within a single fleeting area, the security assessments of facilities and towing vessels should include the barge sizes and cargos that would result in a worst-case scenario (i.e. greatest potential consequence due to cargo volatility, toxicity, or environmental damage), and the most probable vulnerability scenarios.

Vessel and facility security plans must address how the vessel or facility will apply the necessary security measures when engaged with a barge.