

nationwide consistency to strengthen maritime security without putting any particular State or region at a competitive economic disadvantage. We believe, however, that local security considerations are imperative in security plans. Our regulations do not mandate specific security measures; rather, they require the development and implementation of security assessments and plans. It is possible that security measures taken to date to fulfill State or local requirements will be sufficient to meet the new Federal requirements. These security measures may be accounted for in security assessments and should be fully documented in the security plans submitted to the Coast Guard. Local COTPs, who will review Facility Security Assessment reports and Facility Security Plans submitted under part 105, will be able to assess compliance and alignment with local, State, and Federal requirements.

One commenter asked for clarification of the terms "self assessments," "security assessments," "risk/threat assessments," and "on-scene surveys."

Risk/threat assessments and self assessments are not specifically defined in the regulations, but refer to the general practices of assessing where a vessel or facility is at risk. The assessments required in parts 104 through 106 must take into account threats, consequences, and vulnerabilities; therefore, they are most appropriately titled "security assessments." This title also aligns with the ISPS Code. To clarify that §§ 101.510 and 105.205 address security assessments required by subchapter H, we have amended these sections to change the term "risk" to the more accurate term "security." "On-scene surveys" are explained in the security assessment requirements of parts 104, 105, and 106. As explained in § 104.305(b), for example, the purpose of an on-scene survey is to "verify or collect information" required to compile background information and "consists of an actual survey that examines and evaluates existing vessel protective measures, procedures, and operations." An on-scene survey is part of a security assessment.

One commenter stated that if a Facility Security Assessment determines a threat that is outside the scope of what is appropriate to include in the Facility Security Plan, the threat should be included as part of the AMS Plan.

We agree with the commenter. The AMS Plan is more general in nature and takes into account those threats that may affect the entire port, or a segment of the port. As such, the AMS Plan

should be designed to take into account those threats that are larger in scope than those threats that should be considered for individual facilities. To focus the Facility Security Assessments on their port interface rather than the broader requirement, we have amended §§ 105.305 (c)(2)(viii), (ix) and 106.305 (c)(2)(v) to reflect that the assessment of the facility should take into consideration the use of the facility as a transfer point for a weapon of mass destruction and the impact of a vessel blocking the entrance to or area surrounding a facility. Two commenters addressed the requirements of analyzing a facility's threats under § 105.305(c)(2) and (c)(3). One commenter said that the analysis of threats required by § 105.305(c)(2) and (c)(3) should be addressed in the AMS Plan and not in the Facility Security Plan because threat assessment is a government responsibility. One commenter stated that the analysis of threat information should not be required in the Facility Security Assessment because the government is best situated to assess threats.

We agree that threat analysis is part of the AMS Plan. However, a facility's security also depends in large part on how well the owner or operator assesses vulnerabilities that only he or she would know about and the consequences that could occur from the unique operations or location of the facility, as well as on the assessment of threats identified by the government. The facility's own assessment is imperative to the development of the Facility Security Plan that must identify these unique aspects and address them in a manner appropriate for the facility. Threat information, which will be issued by the Coast Guard or other agencies having knowledge of this type of information, should be considered in the Facility Security Assessment. In general, however, lacking specific threat assessment information, the facility owner or operator must assume that threats will increase against the vulnerable part of the facility and develop progressively increasing security measures, as appropriate.

Three commenters asked how a company should assess the "worse-case scenario" regarding barges and their cargo.

There are various methods of conducting a security assessment, several of which we outlined in § 101.510. These assessment tools, the assessment requirements themselves as discussed in §§ 104.305, 105.305, and 106.305, and other assessment tools that have been developed by industry should enable owners or operators to evaluate

the vulnerability and potential consequences of a transportation security incident involving the barge or the cargo it carries.

Three commenters noted that vulnerability assessments should take into account the type of cargo handled or transported, especially if the cargo is CDC. One commenter stated that CDCs should be carefully considered. One commenter stated that the Coast Guard should also take into account the type of cargo handled during our review of a Facility Security Assessment and Plan. One commenter noted that there is a lower risk associated with Great Lakes facilities that primarily handle dry-bulk cargoes.

We agree that security assessments and security plans should take into account the type of cargo that is handled to maximize the focus of security efforts. During our review of all assessments and plans, the Coast Guard will take into consideration types of cargo handled or transported.

After further review of subpart C of parts 104, 105, and 106, we noted the omission of detailing when the security assessment must be reviewed. Therefore, we are amending §§ 104.310, 105.310, and 106.310 to state that the security assessment must be reviewed and updated each time the security plan is revised and when the security plan is submitted for re-approval.

Two commenters asked for clarification regarding the reference to § 105.415, "Amendment and audit," found in § 105.310(a).

We reviewed § 105.310(a) and have corrected the reference to read "§ 105.410." We meant for the Facility Security Assessment report to be included with the Facility Security Plan when that plan is submitted to the Coast Guard for approval under § 105.410. We are also amending §§ 105.415 and 106.310 to make similar corrections to references.

Subpart D—Facility Security Plan (FSP)

This subpart describes the content, format, and processing requirements for Facility Security Plans.

We received five comments asking which entity, the owner or operator, assumes responsibility for compliance and facility security. Two commenters noted that multiple companies may temporarily lease a "dock facility," and questioned if each is required to submit a Facility Security Plan along with the "dock owner." One commenter stated that the landlord of a facility should develop and implement a security plan and the tenants at the facility should be included in the landlord's plan. One commenter believed that 33 CFR part