

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.

We received four comments regarding the use of third party companies to conduct security assessments. Two commenters asked if we will provide a list of acceptable assessment companies because of the concern that the vulnerability assessment could “fall into the wrong hands.” One commenter requested that the regulations define “appropriate skills” that a third party must have in order to aid in the development of security assessments. One commenter stated that the person or company conducting the assessment might not be reliable.

We will not be providing a list of acceptable assessment companies, nor will we define “appropriate skills.” It is the responsibility of the vessel or facility owner or operator to vet companies that assist them in their security assessments. In the temporary interim rule (68 FR 39254) (part 101), we stated, “we reference ISPS Code, part B, paragraph 4.5, as a list of competencies all owners and operators should use to guide their decision on hiring a company to assist with meeting the regulations. We may provide further guidance on competencies for maritime security organizations, as necessary, but do not intend to list organizations, provide standards within the regulations, or certify organizations.” We require security assessments to be protected from unauthorized disclosures

and will enforce this requirement, including through the penalties provision under § 101.415.

After further review of subpart C of parts 104, 105, and 106, 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 reapproval.

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—Outer Continental Shelf (OCS) Facility Security Plan (FSP)

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

One commenter recommended that the interval for audits of the OCS Facility Security Plan be changed to biennial to be consistent with the audit requirements for emergency response plans.

The annual audit certifies that the OCS Facility Security Plan continues to meet the applicable requirements of part 106. We believe that annual audits are necessary because the OCS Facility Security Plan, as a living document, should be continuously updated to incorporate changes or lessons learned from drills and exercises.

Three commenters recommended that this rule be amended to close “the gap” in the plan-approval process to address the period of time between December 29, 2003, and July 1, 2004. Another commenter suggested submitting the Facility Security Plan for review and approval for a new facility “within six months of the facility owner or operator’s intent of operating it.”

We agree that the regulations do not specify plan-submission lead time for vessels, facilities, and OCS facilities that come into operation after December 29, 2003, and before July 1, 2004. The owners or operators of such vessels, facilities, and OCS facilities are responsible for ensuring they have the necessary security plans submitted and approved by July 1, 2004, if they intend to operate. We have amended §§ 104.410, 105.410, and 106.410 to clarify the plan-submission

requirements for the various dates before July 1, 2004, and after this date.

Thirty commenters commended the Coast Guard for providing an option for an Alternative Security Program as described in § 101.120(b) and urged the Coast Guard to approve these programs as soon as possible.

We believe the provisions in § 101.120(b) will provide greater flexibility and will help owners and operators meet the requirements of these rules. We will review Alternative Security Program submissions in a timely manner to determine if they comply with the security regulations for their particular segment. Additionally, we have amended §§ 104.410(a)(2), 105.115(a), 105.410(a)(2), 106.110(a), and 106.410(a)(2), to clarify the submission requirements for the Alternative Security Program.

After further review of the “Submission and approval” requirements in §§ 101.120, 104.410, 105.410, and 106.410, we have amended the requirements to clarify that security plan submissions can be returned for revision during the approval process.

We received 15 comments about the process of amending and updating the security plans. Five commenters requested that they be exempted from auditing whenever they make minimal changes to the security plans. Two commenters stated that it should not be necessary to conduct both an amendment review and a full audit of security plans upon a change in ownership or operational control. Three commenters requested a *de minimis* exemption to the requirement that security plans be audited whenever there are modifications to the vessel or facility. Seven commenters stated that the rule should be revised to allow the immediate implementation of security measures without having to propose an amendment to the security plans at least 30 days before the change is to become effective. The commenters stated that there is something “conceptually wrong” with an owner or operator having to submit proposed amendments to security plans for approval when the amendments are deemed necessary to protect vessels or facilities.

The regulations require that upon a change in ownership of a vessel or facility, the security plan must be audited and include the name and contact information of the new owner or operator. This will enable the Coast Guard to have the most current contact information. Auditing the security plan is required to ensure that any changes in personnel or operations made by the new owner or operator do not conflict with the approved security plan. The