

in 49 CFR part 1520. These regulations state that information designated as sensitive security information may not be shared with the general public. FOIA exempts from its mandatory release provisions those items that other laws forbid from public release. Thus, security assessments, security assessment reports, and security plans, which should be designated as sensitive security information, are all exempt from release under FOIA.

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), 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, in § 101.415.

Six commenters suggested that a template for security assessments and plans be provided for affected entities. One commenter specifically asked for guidance templates for barge fleeting facilities.

We intend to develop guidelines for the development of security assessments and plans. Additionally, the regulations allow owners and operators of facilities and vessels to implement Alternative Security Programs. This would allow owners and operators to participate in a development process with other industry groups, associations, or organizations. We anticipate that one such Alternative Security Program will

include a template for barge fleeting facilities.

One commenter requested that we allow a group of facilities that combine to act as an identified unit to be considered as an equivalency or add a definition of either "port" or "port authority." The commenter also stated that part 105 should allow port security plans, developed by local government port authorities and approved by State authorities, to serve as equivalent security measures.

We do not agree with adding a definition of "port" to recognize a group of facilities that combine to act as an identified unit. However, groups of facilities may work together to enhance their collective security and achieve the performance standards in the regulations. Locally developed port security plans may serve as an excellent starting point for those facilities located within the jurisdiction of a port authority. We believe that the provisions of §§ 105.300(b), 105.310(b), and 105.400(a) permit the COTP to approve a Facility Security Plan that covers multiple facilities, such as a co-located group of facilities that share security arrangements, provided that the particular aspects and operations of each subordinate facility are addressed in the common assessment and security plan. A single Facility Security Officer for the port or port cooperative should be designated to facilitate this common arrangement. Finally, local security programs developed by entities such as a port authority or a port cooperative may be submitted to the Coast Guard for consideration as Alternative Security Programs in accordance with § 101.120(c).

Four commenters requested that the Company and the Facility Security Officers be given access to the "vulnerability assessment" done by the COTP to facilitate the development of the Facility Security Plan and ensure that the Facility Security Plan does not conflict with the AMS Plan.

The AMS Assessments directed by the Coast Guard are broader in scope than the required Facility Security Assessments. The AMS Assessment is used in the development of the AMS Plan, and it is a collaborative effort between Federal, State, Indian Tribal and local agencies as well as vessel and facility owners and operators and other interested stakeholders. The AMS Assessments are sensitive security information. Access to these assessments, therefore, is limited under 49 CFR part 1520 to those persons with a legitimate need-to-know (e.g., Facility Security Officers who need to align Facility Security Plans with the AMS

Plan may be deemed to have need to know sensitive security information). In addition, the Coast Guard will identify potential conflicts between security plans and the AMS Plan during the Facility Security Plan approval process.

Five commenters were concerned about the ability of private industry to assess threats. One commenter asked that we change § 105.300(d)(1) to read "known security threats and known patterns," stating that private industry has not been provided detailed knowledge on security threats and patterns. One commenter stated that vessels and facilities are not capable of determining their risks because they lack knowledge about the activities of individuals seeking to do harm from locations off the vessel or facility. One commenter asserted that scenarios "outside the domain of control" of a vessel or facility owner or operator cannot be countered by private industry, and stated that the expertise requirement for those conducting risk assessments should be suggested, not mandatory. One commenter stated that industry should not be required to address mitigation strategies for chemical, nuclear, or biological weapons because they lack the necessary expertise.

The intent of § 105.300(d)(1) is that those facility personnel involved in conducting the Facility Security Assessment should have expertise in security threats and patterns or be able to draw upon third parties who have this expertise. Amending the language as suggested is not necessary because, as allowed in § 105.300(c), the Facility Security Officer may use third parties in any aspect of the Facility Security Assessment if that party has the appropriate skills and knowledge. Expertise in assessing risks is crucial for establishing security measures to accurately counter the risks, and therefore we believe that expertise is required.

One commenter requested that local agencies, rather than the Coast Guard, analyze security requirements, stating that his company has already spent a considerable amount of money complying with local standards.

We disagree that local agencies should have the sole responsibility to review, approve, and ensure implementation of security measures as required under part 105. The MTSA gave the Coast Guard the authority to require areas, vessels, and facilities to implement security measures. We do not intend to delegate this authority to State or local agencies because we believe the system, as mandated by the MTSA, provides the necessary