

“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 seven comments regarding waivers, equivalencies, and alternatives. Three commenters appreciated the flexibility of the Coast Guard in extending the opportunity to apply for a waiver or propose an equivalent security measure to satisfy a specific requirement. Four commenters requested detailed information regarding the factors the Coast Guard will focus on when evaluating applications for waivers, equivalencies, and alternatives.

The Coast Guard believes that equivalencies and waivers provide flexibility for vessel owners and operators with unique operations. Sections 104.130, 105.130, and 106.125 state that vessel or facility owners or operators requesting waivers for any requirement of part 104, 105, or 106 must include justification for why the specific requirement is unnecessary for that particular owner's or operator's vessel or facility or its operating conditions. Section 101.120 addresses Alternative Security Programs and § 101.130 provides for equivalents to security measures. We intend to issue guidance that will provide more detailed information about the application procedures and requirements for waivers, equivalencies, and the Alternative Security Program.

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 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).

Six commenters asked that terms and definitions in the regulations match those in the ISPS Code, and not the terms and definitions in the MTSA, to minimize confusion among international companies. Two commenters stated that inclusion of the ISPS Code terms “port facility security plan” and “port facility security officer” in the definitions of AMS Plan and Federal Maritime Security Coordinator, respectively, in these regulations will cause confusion and is contrary to the intent of the ISPS Code.

We recognize that it can be confusing for foreign flag vessels to operate under different definitions than those present in the ISPS Code. The ISPS Code, however, gives contracting governments latitude in implementing its provisions. At the same time, the MTSA imposes its own requirements. Our regulations align the requirements of both the ISPS Code and the MTSA, and the definitions used within the regulations reflect this alignment.

We received several comments that were beyond the scope of this final rule. One commenter supported making foreign flag vessel owners, operators, and vessel managers financially accountable for the direct and indirect economic impacts resulting from a terrorist activity stemming from one of their company's managed commercial vessels. One commenter asked that their product be included as part of these final rules.

Imposing these suggested financial obligations is beyond the scope of this final rule. There are, however, new provisions such as the continuous synopsis record (SOLAS Chapter XI-1, regulation 5) that effectively address ownership and identify those that may be responsible for the operation of the vessel. Product solicitations are also beyond the scope of this final rule and are not addressed.

Three commenters questioned the foreign port assessment program. One commenter stated the U.S. assessment of foreign ports could create “too many layers” of inspection, stating that the European Commission will assess the security of their own ports, and the U.S.

assessment process is, therefore, duplicative. Two commenters recommended that the U.S. accept assessments of foreign ports by reputable maritime administrations in accordance with IMO requirements. One commenter expressed concerns regarding the Coast Guard's intention to conduct foreign port audits, and expressed hope that the U.S. would accept the International Labor Organization's (ILO) work on seafarer credentialing.

The Coast Guard, in cooperation with TSA, BCBP, and MARAD, is still developing the foreign port assessment program to implement 46 U.S.C. 70108. We intend to work cooperatively with officials in foreign ports and other organizations, such as the European Commission and ILO, to reduce unnecessary duplication in assessing the effectiveness of antiterrorism measures maintained at foreign ports and the credentialing of seafarers.

Subpart B—Maritime Security (MARSEC) Levels

This subpart concerns the setting of MARSEC Levels.

We received 15 comments regarding MARSEC Level alignment. One commenter agreed with the alignment. One commenter stated that §§ 101.200 and 101.205 are inconsistent with one another. Six commenters stated that problems are likely to arise because MARSEC Levels do not match other Federal threat levels, such as the Homeland Security Advisory System (HSAS).

We disagree with the dissenting commenters. Section 101.200(d) states that COTPs may temporarily raise the MARSEC Level for their specific areas of responsibility when necessary to address an exigent circumstance immediately affecting the security of the maritime elements of their areas of responsibility. This is a narrow set of circumstances; we expect national MARSEC Levels to be established at the level of the Commandant, as stated in § 101.205. Additionally, as stated in § 101.205, MARSEC Levels have been aligned with DHS's HSAS.

In reviewing Table 101.205, we noted that the reference to the Blue HSAS threat condition should be “guarded” and reference to the Yellow HSAS threat condition should be “elevated.” We have amended Table 101.205 to reflect this clarification.

Subpart C—Communication (Port-Facility-Vessel)

This subpart concerns the communication of MARSEC Levels, threats, confirmations of attainment,