

narrow than that contained in the General Provisions of part 101.

In section 101.115 we have incorporated by reference the ISPS Code, 2003 Edition. Specifically, we are incorporating the amendments adopted on 12 December 2002 to the Annex to The International Convention for SOLAS, 1974 and the ISPS Code, parts A and B, also adopted on 12 December 2002. The material is incorporated for all of subchapter H.

Sections 101.120 and 101.125 of subpart A reflect the flexibility that the Coast Guard has tried to build into these regulations. Section 101.120(a) reflects one of the SOLAS amendments, and allows the U.S. to agree upon alternative security arrangements with other SOLAS contracting governments, but only to cover short, international voyages on fixed routes between facilities subject to the jurisdiction of the U.S. and facilities subject to the jurisdiction of the other contracting government. Any vessel covered by one of the agreements is prohibited from engaging in any vessel-to-vessel activity, unless it would be conducting the vessel-to-vessel activity with another vessel covered by the same agreement.

Section 101.120(b)–(c) allows applications for approval of Alternative Security Programs. As noted in the discussion of comments section above, we received many comments supporting the idea of allowing vessels or facilities to submit security plans or programs that meet, as an example, an industry standard, instead of requiring them to follow the plan requirements included

in this subchapter, SOLAS, or ISPS Code, parts A and B. We have, accordingly, built this flexibility into the regulation. Once an Alternative Security Program is approved, it will be added to Section 101.125. An up-to-date list will also be kept by G–MP, and will be accessible on the Internet.

Section 101.120(c) details the information that must be included in an application for approval. Part of that application includes an assessment of what vessels or facilities may use the proposed Alternative Security Program. This is important because not all Alternative Security Program will be appropriate for all vessels or facilities. For example, not all approved Alternative Security Programs for facilities will fit the security planning requirements necessary for a CDC facility. As part of the approval process, the Commandant will indicate, in his approval letter, those types of vessels or facilities that may use the approved Alternative Security Programs.

Section 101.130 allows the Commandant to accept equivalent security measures, so long as they are at least as effective as those that are mandated in subchapter H, SOLAS, or ISPS Code, parts A and B. This allowance is made for both vessels and facilities required to have security programs under parts 104, 105, or 106. Equivalent security measures differ from Alternative Security Programs. Once an Alternative Security Program is approved, any vessel or facility that meets the approval qualifications may

meet the provisions of the Alternative Security Program in lieu of meeting the security plan requirements of the applicable part of this subchapter. Equivalent security measures, once approved, are only approved for the particular vessel or facility making the application.

Equivalent security measures are those distinct security measures, such as fences or alarm systems, which may be required within a security plan. Requests for approval of equivalent security measures should be made at the time that a vessel or facility is submitting their security plan for approval, and they should be made to the appropriate plan approval authority under part 104, 105, or 106.

Part 101—Subpart B—Maritime Security Levels

The SOLAS Amendments and ISPS Code lay out a series of requirements for Contracting Governments and Administrations to mandate security levels that are appropriate for their vessels and ports. The Coast Guard is implementing these requirements in coordination with the HSAS. Homeland Security Presidential Directive (HSPD)–3 defines a five-tiered system for setting threat levels. We are implementing MARSEC Levels, which directly correspond to the security levels as discussed in the SOLAS amendments and the ISPS Code. The MARSEC Levels will be linked to the HSAS as shown in the table below. This table is also included in the regulation itself.

TABLE 5.—RELATION BETWEEN HSAS, MARSEC LEVELS AND SOLAS-REQUIRED SECURITY LEVELS

Homeland security advisory system (HSAS) threat condition	Equivalent maritime security (MARSEC) level	Equivalent SOLAS-required security level
Low: Green Elevated: Blue Guarded: Yellow	Maritime Security Level 1	Security Level 1.
High: Orange	Maritime Security Level 2	Security Level 2.
Severe: Red	Maritime Security Level 3	Security Level 3.

At all times, the Commandant retains the discretion to adjust the MARSEC Level when necessary to address any particular concerns or circumstances related to the maritime elements of the national transportation system. Additionally, the COTP retains the authority to temporarily raise the MARSEC Level for his/her AOR, or a specific segment thereof, when necessary to address exigent circumstances immediately affecting the security of the maritime elements of the

national transportation system within his/her AOR.

Part 101—Subpart C—Communication

Subpart C, section 101.300 details the methods the COTP will use to communicate changes in the MARSEC Level. Note that individual ATMS Plans may outline additional communication methods that are particular to the Plan's covered area. It also details the threat information that the COTP will, when appropriate, communicate to the port stakeholders, vessels, and facilities

located within his or her AOR. Finally, this section requires vessel and facility security plan holders to confirm that they have implemented the measures and/or actions in their security plans that correspond to the MARSEC Level.

Subpart C, section 101.305 describes the reporting requirements placed on vessel and facility security plan holders. First, it requires that they report suspicious activities that may result in a transportation security incident. These reports are to be made to the National Response Center (NRC), and the