

in SOLAS Chapter XI-2, Regulation 10, and the ISPS Code. The timing requirements for the Declaration of Security are specified §§ 104.255 and 105.245. The format for a Declaration of Security can be found as an appendix to the ISPS Code. We agree that the format requirement was not clearly included in § 101.505(a) when we called out the incorporation by reference. Therefore, we have explicitly included a reference to the format in § 101.505(b).

One commenter wanted to know who will become the arbiter in the event of a disagreement between a vessel and a facility, or between two vessels, in regards to the Declaration of Security.

We do not anticipate this will be a frequent problem. The regulations do not provide for or specify an arbiter in the event that an agreement cannot be reached for a Declaration of Security. It is important to note that failure to resolve any such disagreement prior to the vessel-to-facility interface may result in civil penalties or other sanctions.

Five commenters urged us to exempt offshore supply vessels and the facilities or OCS facilities they interact with from the Declaration of Security requirements because they do not pose a higher risk to persons, property, or the environment.

We disagree with the commenters, and we believe that the regulated vessels and the facilities that they interface with may be involved in a transportation security incident. In addition, Declarations of Security ensure essential security-related coordination and communication among vessels and OCS facilities.

One commenter asked whether the Declaration of Security requirement applies to vessel-to-vessel activity or vessel-to-facility interfaces beyond the 12-mile limit but still in the U.S. Exclusive Economic Zone (EEZ).

Vessel-to-vessel activity in the EEZ is not included in these regulations, except if one of the vessels is intending to enter a U.S. port. The regulations do apply to vessels interfacing with OCS facilities.

One commenter stated that the Declaration of Security procedures could put vessels at a competitive disadvantage when dealing with a facility that may demand that vessels pay for all the security. The commenter suggested that the Coast Guard act as arbiter when disputes arise between facilities and vessels concerning who is responsible for specific security measures.

The fundamental intent of these regulations is to establish cooperation and communication between owners and operators of facilities and vessels to

minimize the potential for a transportation security incident. A facility that places the onus on vessels to provide all the security would be acting contrary to the regulations. When approving security plans, the COTP has the discretion to determine whether a facility has implemented sufficient security measures to meet the requirements of these regulations. Any agreements or mandates that the facility owner or operator intends to prescribe to vessels should be reflected in the Facility Security Plan.

Five commenters recommended that § 104.255(b)(1), (b)(2), and (c) be amended so that the security arrangements required by this section may be arranged "on or prior to" rather than "prior to." One commenter recommended that we amend § 104.255(c) to waive the Declaration of Security requirements except in cases where the duration of the interface will exceed 3 hours.

We believe that it is important for the Vessel Security Officer and the Facility Security Officer to be in communication "prior" to the vessel's arrival at the facility. Using a lower standard of "on or prior to" may not ensure that all the necessary security measures will be in place at the vessel's arrival. Therefore, we did not make the amendment to the language in paragraphs (b)(1) or (b)(2) of this section. However, we are amending § 104.255(c) and (d) so that the Vessel Security Officer and the Facility Security Officer can coordinate security needs and procedures, and agree upon the contents of the Declaration of Security for the interface. The signing of the Declaration of Security can occur upon interface. We do not intend to waive any of the Declaration of Security requirements for interfaces during higher MARSEC levels. The changes to § 104.255(c) and (d) align the procedures for Declaration of Security at each MARSEC Level. We also amended the language in § 104.255(b)(2) to clarify that this paragraph applies to the period of time for the vessel-to-vessel activity.

Two commenters stated that it is confusing as to whether a vessel not carrying CDC must provide a Declaration of Security at a facility or another vessel's request until MARSEC Level 2.

At MARSEC Level 1, only cruise ships and vessels certificated to carry CDC are required to establish a Declaration of Security. At MARSEC Levels 2 and 3, all vessel-to-facility interfaces require a Declaration of Security. Owners and operators may establish continuing Declarations of Security for any vessel in accordance with § 104.255(e)(2) and (e)(3).

One commenter suggested that the Coast Guard establish additional criteria for certain expensive security equipment (*e.g.*, access controls, lighting, and surveillance). The commenter said this would be helpful in ensuring a minimum compliance standard for those equipment elements that will be most costly to owners and operators.

Our regulations set performance standards. Some industry standards already exist or are being developed by trade or standards-setting organizations. Owners and operators may assess their own security needs and the measures that best meet those needs, given the particular characteristics and unique operations of their vessels and facilities.

Seven commenters suggested that, instead of requiring disciplinary measures to discourage abuse of identification systems, the Coast Guard should merely require companies to develop policies and procedures that discourage abuse. One commenter opposed provisions of these rules relating to identification checks of passengers and workers. The commenter stated that these provisions threaten constitutional rights to privacy, travel, and association, and are too broad for their purpose. The commenter argued that identification methods are inaccurate or unproven and can be abused, and that the costs of requiring identification checks outweigh the proven benefit.

We recognize the seriousness of the commenters' concerns, but disagree that provisions for checking passenger and worker identification should be withdrawn. Identification checks, by themselves, may not ensure effective access control, but they can be critically important in attaining access control. Our rules implement the MTSA and the ISPS Code by requiring vessel and facility owners and operators to include access control measures in their security plans. However, instead of mandating uniform national measures, we leave owners and operators free to choose their own access control measures. In addition, our rules contain several provisions that work in favor of privacy. Identification systems must use disciplinary measures to discourage abuse. Owners and operators can take advantage of rules allowing for the use of alternatives, equivalents, and waivers. Passenger and ferry vessel owners or operators are specifically authorized to develop alternatives to passenger identification checks and screening. Signage requirements ensure that passengers and workers will have advance notice of their liability for screening or inspection. Vessel owners