(s) The jurisdiction of Federal, State, Indian Tribal, and local government agencies and law enforcement entities over area security related matters;

* * * * *

(w) Identification of any facility otherwise subject to part 105 of this subchapter that the COTP has designated as a public access facility within the area, the security measures that must be implemented at the various MARSEC Levels, and who is responsible for implementing those measures.

■ 7. In § 103.515—

■ a. In paragraph (a), after the word ''conduct'', add the words ''or participate in''; and

■ b. Revise paragraph (c) to read as follows:

**§ 103.515 Exercises.**

* * * * *

(c) Upon review by the cognizant District Commander, and approval by the cognizant Area Commander, the requirements of this section may be satisfied by—

(1) Participation of the COTP and appropriate AMS Committee members or other appropriate port stakeholders in an emergency response or crisis management exercise conducted by another governmental agency or private sector entity, provided that the exercise addresses components of the AMS Plan;

(2) An actual increase in MARSEC Level; or

(3) Implementation of enhanced security measures enumerated in the AMS Plan during periods of critical port operations or special marine events.

Dated: October 8, 2003.

**Thomas H. Collins,**

*Admiral, Coast Guard, Commandant.*

[FR Doc. 03–26346 Filed 10–20–03; 8:45 am]

**BILLING CODE 4910–15–U**

---

## DEPARTMENT OF HOMELAND SECURITY

## Coast Guard

## 33 CFR Parts 104, 160, and 165

## 46 CFR Parts 2, 31, 71, 91, 115, 126, and 176

**[USCG–2003–14749]**

**RIN 1625–AA46**

## Vessel Security

**AGENCY:** Coast Guard, DHS.

**ACTION:** Final rule.

**SUMMARY:** This final rule adopts, with changes, the temporary interim rule published on July 1, 2003, that provides security measures for certain vessels calling on U.S. ports. It also requires the owners or operators of vessels to designate security officers for vessels, develop security plans based on security assessments and surveys, implement security measures specific to the vessel's operation, and comply with Maritime Security Levels. This rule is one in a series of final rules on maritime security in today's **Federal Register**. To best understand this rule, first read the final rule titled ''Implementation of National Maritime Security Initiatives'' (USCG–2003–14792), published elsewhere in today's **Federal Register**.

**DATES:** This final rule is effective November 19, 2003. On July 1, 2003, the Director of the Federal Register approved the incorporation by reference of certain publications listed in this final rule.

**ADDRESSES:** Comments and material received from the public, as well as documents mentioned in this preamble as being available in the docket, are part of docket USCG–2003–14749 and are available for inspection or copying at the Docket Management Facility, U.S. Department of Transportation, room PL–401, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet at *http://dms.dot.gov*.

**FOR FURTHER INFORMATION CONTACT:** If you have questions on this final rule, call Lieutenant Commander Darnell Baldinelli (G–MPS), U.S. Coast Guard by telephone 202–267–4148 or by electronic mail *dbaldinelli@comdt.uscg.mil*. If you have questions on viewing the docket, call Andrea M. Jenkins, Program Manager, Docket Operations, Department of Transportation, at telephone 202–366–0271.

**SUPPLEMENTARY INFORMATION:**

### Regulatory Information

On July 1, 2003, we published a temporary interim rule with request for comments and notice of public meeting titled ''Vessel Security'' in the **Federal Register** (68 FR 39292). This temporary interim rule was one of a series of temporary interim rules on maritime security published in the July 1, 2003, issue of the **Federal Register**. On July 16, 2003, we published a document correcting typographical errors and omissions in that rule (68 FR 41915).

We received a total of 438 letters in response to the six temporary interim rules by July 31, 2003. The majority of these letters contained multiple comments, some of which applied to the docket to which the letter was submitted, and some of which applied to a different docket. For example, we received several letters in the docket for the temporary interim rule titled ''Implementation of National Maritime Security Initiatives'' that contained comments in that temporary interim rule, plus comments on the ''Vessel Security'' temporary interim rule. We have addressed individual comments in the preamble to the appropriate final rule. Additionally, we had several commenters submit the same letter to all six dockets. We counted these duplicate submissions as only one letter, and we addressed each comment within that letter in the preamble for the appropriate final rule. Because of statutorily imposed time constraints for publishing these regulations, we were unable to consider comments received after the period for receipt of comments closed on July 31, 2003.

A public meeting was held in Washington, DC, on July 23, 2003, and approximately 500 people attended. Comments from the public meeting are also included in the ''Discussion of Comments and Changes'' section of this preamble.

In order to focus on the changes made to the regulatory text since the temporary interim rule was published, we have adopted the temporary interim rule and set out, in this final rule, only the changes made to the temporary interim rule. To view a copy of the complete regulatory text with the changes shown in this final rule, *see http://www.uscg.mil/hq/g-m/mp/index.htm.*

### Background and Purpose

A summary of the Coast Guard's regulatory initiatives for maritime security can be found under the ''Background and Purpose'' section in the preamble to the final rule titled ''Implementation of National Maritime Security Initiatives'' (USCG–2003–14792), published elsewhere in this issue of the **Federal Register**.

### Impact on Existing Domestic Requirements

33 CFR part 120, Security of Vessels, currently exists but applies only to cruise ships. Until July 2004, 33 CFR part 120 will remain in effect. Vessels that were required to comply with part 120 must now also meet the requirements of this part, including § 104.295, Additional requirements—cruise ships. The requirements in § 104.295 generally capture the existing requirements in part 120 that are specific for cruise ships and capture additional detail to the requirements of

the International Convention for the Safety of Life at Sea, 1974, (SOLAS) Chapter XI–2 and the International Ship and Port Facility Security Code (ISPS Code).

**Discussion of Comments and Changes**

Comments from each of the temporary interim rules and from the public meeting held on July 23, 2003, have been grouped by topic and addressed within the preambles to the applicable final rules. If a comment applied to more than one of the six rules, we discussed it in the preamble to each of the final rules that it concerned. For example, discussions of comments that requested clarification or changes to the Declaration of Security procedures are duplicated in the preambles to parts 104, 105, and 106. Several comments were submitted to a docket that included topics not addressed in that particular rule, but were addressed in one or more of the other rules. This was especially true for several comments submitted to the docket of part 101 (USCG–2003–14792). In such cases, we discussed the comments only in the preamble to each of the final rules that concerned the topic addressed.

*Subpart A—General*

This subpart contains provisions concerning applicability, waivers, and other subjects of a general nature applicable to part 104.

One commenter asked the Coast Guard to clarify the difference between ''vessel-to-vessel activity,'' as defined in § 101.105, and ''vessel-to-vessel interface,'' as used in part 104.

We find that the terms ''vessel-to-vessel activity'' and ''vessel-to-vessel interface'' are comparable and have chosen to use the term ''vessel-to-vessel activity'' to align these regulations with the ISPS Code. We have amended the definition of ''Declaration of Security'' in § 101.105 as well as §§ 104.255 and 104.300 to use the term ''vessel-to-vessel activity'' in place of ''vessel-to-vessel interface,'' for consistency.

We received 11 comments relating to the use of the terms ''vessel-to-facility interface,'' ''vessel-to-port interface,'' and ''vessel-to-vessel activity.'' Seven commenters requested that the Coast Guard be consistent in its use of ''vessel-to-vessel interface'' in § 101.105 and use the word ''cargo'' instead of the phrase ''goods or provisions.'' One commenter asked us to modify the definition of a ''vessel-to-vessel activity'' to include the transfer of a container to or from a manned or unmanned vessel. One commenter noted that it should be made clear that the term ''vessel-to-facility interface'' refers to when the vessel is at the facility or arriving at the facility.

We partially agree with the commenters. We have amended the definitions for ''vessel-to-facility interface,'' ''vessel-to-port interface,'' and ''vessel-to-vessel activity'' in § 101.105 to use the words ''cargo'' and ''vessel stores'' instead of the word ''goods'' to be clearer for the intended activities. The term ''vessel-to-facility interface'' clearly states that the vessel is either at, or arriving at, the facility, and therefore, we did not amend the definition further.

Two commenters asked that the Coast Guard enumerate the specific categories and thresholds of vessels that are required to comply with the regulations. One commenter stated that it would be helpful if the Coast Guard provided a chart showing what types of vessels are and are not required to comply.

We understand that the applicability of part 104 presumes that a vessel owner or operator is familiar with existing laws and regulations for vessels. We believe this cross-reference to existing law and regulation is the best way to ensure that § 104.105 is clear; therefore, we have not amended the applicability section to include a chart. We have created Small Business Compliance Guides, which may be useful to owners and operators trying to determine the applicability of part 104. These Guides may be found at the locations listed in the ''Assistance for Small Entities'' section of this final rule.

Two commenters requested that § 104.105(b) regarding applicability of parts 101 through 103 for vessels not covered by part 104 be deleted, stating that this language has the effect of making all vessels subject to part 104.

We do not believe that § 104.105(b) has the effect of making all vessels subject to part 104. Paragraph (b) is strictly informational and refers the owner or operator of a vessel not subject to part 104 to parts 101 and 103, to which the owner or operator is subject. A vessel is subject to part 104 only if it is listed in § 104.105(a).

Eleven commenters requested various amendments to § 104.105 regarding specific applicability requirements for vessels, stating that there is no ''general'' applicability of SOLAS, and that Chapter XI–2 should be referenced to narrow the applicability. Two commenters requested that references to foreign or U.S. owned non-self propelled vessels (barges) be included to clarify that applicability is limited to only those barges that carry hazardous or dangerous cargoes.

We agree that the general reference to SOLAS is broad and could encompass more vessels than the applicability in SOLAS, Chapter XI–2. We have amended the reference to the applicability of SOLAS, Chapter XI because subchapter H also addresses those requirements in SOLAS, Chapter XI–1 as well as Chapter XI–2. We also amended § 104.105(a) to clarify that not all non-self-propelled vessels (barges) subject to 33 CFR subchapter I must comply with part 104. We have noted a similar issue with the applicability of part 104 to passenger vessels covered under 46 CFR subchapter K that have overnight accommodations for more than 49 passengers but are not certificated to carry more than 150 passengers. The intent of the applicability for part 104 was not to include these vessels; therefore, we have amended § 104.105(a) to clarify that vessels covered under 46 CFR subchapter K must meet the requirements only if they are certificated to carry more than 150 passengers. In § 104.105(a)(7), we added a clarification that part 104 only applies to vessels on international voyages that carry more than 12 passengers, including at least one passenger-for-hire. We did not include references to foreign or U.S. ownership in all of the applicability paragraphs because it is duplicative to the existing language.

Five commenters recommended changes to the definitions of ''facility'' and ''OCS facility'' in § 101.105 in order to clarify the applicability of parts 104, 105, and 106 to Mobile Offshore Drilling Units (MODUs). Two commenters suggested adding language to the facility definition to specifically include MODUs that are not regulated under part 104, consistent with the definition of OCS facility. Another commenter stated that if we change the definition to include MODUs not regulated under part 104, then we also should add an explicit exemption for these MODUs from part 105. Three commenters suggested deleting the words ''fixed or floating'' and the words ''including MODUs not subject to part 104 of this subchapter'' in § 106.105 and adding a paragraph to read ''the requirements of this part do not apply to a vessel subject to part 104 of this subchapter.''

With regard to the definition of ''facility'' and the suggested additional language regarding MODUs, the definition clearly incorporates MODUs that are not covered under part 104 and MODUs are sufficiently covered under parts 101 through 103 and 106. Therefore, we are not amending our definition of facility nor incorporating the suggested explicit exemption from part 105 because these MODUs are excluded. We have, however, amended

the applicability section of part 104 (§ 104.105) so that foreign flag, non-self propelled MODUs that meet the threshold characteristics set for OCS facilities are regulated by 33 CFR part 106, rather than 33 CFR part 104. We have done so because MODUs act and function more like OCS facilities, have limited interface activities with foreign and U.S. ports, and their personnel undergo a higher level of scrutiny to obtain visas to work on the Outer Continental Shelf. These amendments to § 104.105 required us to add a definition for ''cargo vessel'' in § 101.105. With these changes, we believe the existing definitions of ''facility'' and ''OCS facility'' in § 101.105 are sufficient to conclusively identify those entities that are subject to parts 104, 105, and 106. In addition, the definition of ''OCS facility,'' as written, ensures that these entities will be subject to relevant elements of an OCS Area Maritime Security (AMS) Plan. We believe the language in § 106.105, read in concert with the amended § 104.105(a)(1), and the existing definitions in part 101, is sufficient to preclude MODUs that are in compliance with part 104 from being subject to part 106.

Two commenters stated that our definition of ''international voyage'' includes voyages made by vessels that solely navigate the Great Lakes and St. Lawrence River. The commenter contended that SOLAS specifically exempts vessels that navigate in this area from all the requirements of SOLAS.

We are aware that vessels on the Great Lakes and St. Lawrence Seaway, which are otherwise exempted from SOLAS, are required to comply with our regulations. We have amended the definition of ''international voyage'' in § 101.105 to make this clear. We do not believe that we can require lesser security measures for certain geographic areas, such as the Great Lakes and the St. Lawrence Seaway, and still maintain comparable levels of security throughout the maritime domain. In addition, while SOLAS does not typically apply to the Great Lakes and St. Lawrence Seaway, it allows contracting governments to determine appropriate applicability for their national security. For the U.S., the Maritime Transportation Security Act of 2002 (MTSA) does not exempt geographic areas from maritime security requirements. If vessel owners or operators believe that any vessel security requirements are unnecessary due to their operating environment, they may apply for a waiver under the procedures allowed in § 104.130. Additionally, vessel owners or operators may submit for approval an Alternative Security Program to apply to vessels that operate solely on the Great Lakes and St. Lawrence Seaway.

One commenter asked whether Canadian commercial vessels, greater than 100 gross register tons, operating solely on the Great Lakes will be required to submit their plans to the Coast Guard for approval.

Under § 104.105, all foreign vessels not carrying an approved International Ship Security Certificate (ISSC) intending to enter a port or place subject to jurisdiction of the U.S. are required to submit to the Coast Guard a Vessel Security Plan prepared in response to the Vessel Security Assessment, unless they implement an approved Alternative Security Program. This includes Canadian commercial vessels greater than 100 gross register tons, operating solely on the Great Lakes and calling on U.S ports. We have amended § 104.105 to improve its clarity.

One commenter asked who is responsible for compliance with the security measures in the case of a short-term, bareboat charter in which the vessel has been leased for a period of time.

The regulations require the owner or operator of a vessel to submit a Vessel Security Plan. A true bareboat charterer, meeting the definition of ''demise charterer'' in 46 CFR 169.107, would be the owner or operator of the vessel for the purposes of this subchapter, and therefore, would be responsible for the Vessel Security Plan. If the vessel has other, independent operators, then each operator is required to submit a Vessel Security Plan unless the owner submits a plan that encompasses the operations of each operator. The submission of the security plan should be coordinated between the owner and the independent operators. The Coast Guard will take into account issues concerning the individual responsibilities of the operators and the owners when reviewing the security plan.

Two commenters suggested amending the regulatory threshold for passenger vessels. One commenter recommended that passenger vessels inspected under subchapter K and facilities that service subchapter K vessels, be required to comply with the security requirements only when the vessels have more than 149 passengers aboard. The commenter also stated that it is unreasonable for a subchapter K vessel that operates most of the time with fewer than 150 passengers to comply with the same requirements as a vessel that routinely operates with certificated passengers (*e.g.*, 225 passengers). One commenter suggested that the number of passengers be increased from 150 to 500 or, alternatively, that an exemption be added for those with fewer than 500 passengers.

We disagree with the idea of requiring security based solely on actual passenger count, rather than passenger certification level. It is imperative to maritime security that consistent security measures be in place to reduce the risk of a transportation security incident. For passenger vessels, and the facilities that serve passenger vessels, this threshold is the certification level of a passenger vessel rather than its operating level. Lowering security requirements for passenger vessels when they are not carrying their certificated passenger count allows for inconsistent and inadequate implementation of security measures, which can potentially increase risk. Moreover, owners and operators certificate their vessels at passenger thresholds and can re-certificate their vessels to reflect their business practices.

Two commenters urged the Coast Guard to exclude small passenger vessels subject to SOLAS that are also subject to 46 CFR subchapter T from these final rules, stating that our risk assessment for these vessels does not justify the regulatory requirements that apply to larger passenger vessels, and that the Coast Guard exempts vessels subject to subchapter T from some SOLAS provisions due to their size and small passenger capacity.

Our risk assessment showed that vessels making international voyages, including those subject to 46 CFR subchapter T, may be involved in a transportation security incident. While we have been able to grant waivers and equivalencies for some SOLAS safety-related requirements to some small passenger vessels on the basis of their size, passenger capacity, and where they operate, we believe that all vessels on international voyages should be subject to part 104 because of the higher security risks these vessels pose.

We received 14 comments on the applicability for small passenger vessels. Seven commenters supported our decision to treat small passenger vessels in a manner different than large passenger vessels, by not directly regulating small passenger vessels under part 104. Three commenters requested an exemption to the regulations for all uninspected small passenger vessels operating under 46 CFR subchapter C and all inspected small passenger vessels operating domestically under 46 CFR subchapter T. The commenters stated that the vague requirements and references in the regulations make it

difficult for marine charter firms to determine how they must comply with the new regulations. One commenter asked for clarification on whether small passenger vessels under 46 CFR subchapter T were covered by 33 CFR part 104, stating that these vessels should not be included in the final rules. We received two comments specifically requesting that charterboat vessels less than 100 feet or less than 100 gross tons or that carry fewer than 150 passengers be exempt. The commenters also asked if a vessel were certificated, that an endorsement be made on the vessel's certificate of inspection to reflect the exemption. One commenter stated that the regulations should specify if commercial yachts greater than 100 gross register tons are included.

Small passenger vessels in commercial service regulated under 46 CFR subchapter T and uninspected passenger vessels regulated under 46 CFR subchapter C are not directly regulated in part 104, other than those vessels on international voyages. Therefore, these vessels do not require a specific waiver, exemption, or endorsement. These vessels will be covered, however, in Area Maritime Security (AMS) Assessments and Plans under part 103. Owners, operators, and others associated with these vessels, including charterers, are encouraged to participate—consistent with § 103.300(b) concerning the AMS Committee charter—in the development of the AMS Plan.

We received 64 comments concerned with the application of these security measures to ferries. The commenters did not want airport-like screening measures implemented on ferries, stating that such measures would cause travel delays, frustrating the mass transit aspect of ferry service. The commenters also stated that the security requirements will impose significant costs to the ferry owners, operators, and passengers.

These regulations do not mandate airport-like security measures for ferries; however, ferry owners or operators may have to heighten their existing security measures to ensure that our ports are secure. Ferry owners and operators can implement more stringent screening or access measures, but they can also include existing security measures in the required security plan. These measures will be fully reviewed and considered by the Coast Guard to ensure that they cover all aspects of security for periods of normal and reduced operations.

We understand that ferries often function as mass transit and we have included special provisions for them. Even with these provisions, our cost analysis indicated that compliance with these final rules imposes significant costs to ferry owners and operators. To address this concern, the Department of Homeland Security (DHS) has developed a grant program to provide funding for security upgrades. Ferry terminal owners and operators can apply for these grants.

Nine commenters disagreed with the applicability criteria for towing vessels and barges, manned or unmanned, in the security requirements. Three commenters disagreed with including all towing vessels over 8 meters in length that tow hazardous barges. The commenters stated that security requirements are an undue burden on the harbor industry with little increase in real security. The third commenter recommended that we exempt barges over 10,000 barrels carrying grade D or lower products and towing vessels less than 2,000 horsepower operating exclusively in a harbor. This commenter stated that his vessels do not have the exposure of rotating crews and do not travel out of the port. A fourth commenter said that many towing vessels, not otherwise subject to these regulations, would be included just because they carry ammonium nitrate and no other Certain Dangerous Cargo (CDC) listed under 33 CFR 160.204.

We developed the vessel security requirements to address risks posed by those towing vessels engaged in the transportation of hazardous and dangerous cargoes. These towing vessels and their barges may be involved in a transportation security incident. We believe our focused approach to regulating towing vessels that transport barges with CDC and barges subject to 46 CFR subchapter D or O limits the burden on the towing industry, while increasing maritime security. Even in the case of limited operations, some cargoes are so dangerous that in order to minimize risk, we must regulate vessels carrying those cargoes. It should be noted that when defining what constitutes a CDC, we referenced § 160.204 to ensure consistency in Title 33. We are constantly reviewing and, when necessary, revising the CDC list based on additional threat and technological information. Changes to § 160.204 would affect the regulations in 33 CFR subchapter H because any changes to the CDC list would also affect the applicability of subchapter H. Any such changes would be the subject of a future rulemaking.

Three commenters stated that the Coast Guard needs to describe how it intends to apply these regulations to fleeting and towing operations. The commenters asked how these regulations should be applied to a towing vessel that provides emergency assistance to a regulated barge. The commenters also asked that the Coast Guard describe how it intends to apply the regulations to towing vessels that do not tow regulated cargoes but assist other vessels through locks or narrow bridges. One commenter said that the Declaration of Security provisions in § 104.255(b)(2) should not apply to towing vessels that are providing such assistance.

We have clarified the applicability of part 104 so that some towing vessels, such as assist tugs, assist boats, helper boats, bow boats, harbor tugs, ship-docking tugs, and harbor boats, are not subject to the part because either the primary towing vessel or the facility will be subject to the regulations and will take such assist vessels into account in their security plan. We anticipate that these vessels will engage in operations such as docking, undocking, maneuvering, transiting bridges, transiting locks, pulling cuts through a lock, or assisting in an emergency such as a breakaway barge. This exemption is similar to those used in 46 CFR part 27. Owners or operators of towing vessels not directly regulated under part 104 are covered under parts 101 through 103 and, although there are no specific security measures for assistance towing vessels in these parts, the AMS Plan may call for measures that the assistance towing vessels must follow, or the COTP may require security measures to address specific security concerns. Nothing in these regulations alters any duty that a vessel may have to render assistance to those in distress.

One commenter recommended exempting barges carrying non-hazardous oilfield waste from part 104, stating that they pose little or no security risk and should not be subject to the Vessel Security Plan requirements.

Under § 104.105(a)(8), part 104 applies to all barges subject to 46 CFR subchapters D or O, regardless of their specific cargo. In our risk assessment, we found that vessels subject to subchapter D, including barges carrying non-hazardous oilfield waste, may be involved in a transportation security incident.

Two commenters asked for clarification on which security regulations would apply for self-propelled and non-self-propelled dredges.

If a dredge meets any of the specifications in § 104.105(a), then the

dredge is regulated under part 104. For example, if a dredge's operations include towing a tank barge alongside for bunkers, the dredge must meet the requirements in part 104. If a dredge does not meet any of the specifications in § 104.105(a), then the dredge is covered by the requirements of parts 101 through 103 and, although there are no specific security measures for dredges in these parts, the AMS Plan may call for measures that the dredge must follow, or the COTP may require security measures to address specific security concerns.

Two commenters requested that we broaden the applicability of our vessel security regulations. One commenter stated that the applicability of our vessel security regulations should be broadened to include fishing, recreational, and other vessels less than 100 gross tons. One commenter stated that the regulations should be broadened to include uninspected vessels greater than 100 gross tons.

Our applicability for the security regulations in 33 CFR subchapter H is for all vessels; however, part 104 directly regulates those vessels we have determined may be involved in a transportation security incident. Fishing, recreational, and other vessels less than 100 gross tons are covered by parts 101 through 103 and, although there are no specific security measures for these vessels in these parts, the AMS Plan may set forth measures that will be implemented at the various Maritime Security (MARSEC) Levels that may apply to them.

Two commenters were concerned about the breadth of the regulations. One commenter asked that the regulations be broadened to allow for exemptions. One commenter stated that the applicability as described in § 101.110 is ''much too general,'' stating that it can be interpreted as including a canoe tied up next to a floating dock in front of a private home. The commenter concluded that such a broad definition would generate ''a large amount of'' confusion and discontent among recreational boaters and waterfront homeowners.

Our applicability for the security regulations in 33 CFR subchapter H is for all vessels and facilities; however, parts 104, 105, and 106 directly regulate those vessels and facilities we have determined may be involved in transportation security incidents, which does not include canoes and private residences. For example, § 104.105(a) applies to commercial vessels; therefore, a recreational boater is not regulated under part 104. If a waterfront homeowner does not meet any of the specifications in § 105.105(a), the waterfront homeowner is not regulated under part 105. It should be noted that all waterfront areas and boaters are covered by parts 101 through 103 and, although there are no specific security measures for them in these parts, the AMS Plan may set forth measures that will be implemented at the various MARSEC Levels that may apply to them. Security zones and other measures to control vessel movement are some examples of AMS Plan actions that may affect a homeowner or a recreational boater. Additionally, the COTP may impose measures, when necessary, to prevent injury or damage or to address specific security concerns.

After further review of § 104.110, we recognized that vessels in lay-up status were not addressed. Therefore, we have amended § 104.110 to exempt those that are laid-up, dismantled, or out of commission. This change is consistent with the exemption in part 105 for facilities that receive such vessels.

One commenter stated that the requirements in part 104 are far more prescriptive and onerous than the Coast Guard's guidance previously issued in National Vessel Inspection Circular (NVIC) 10–02, Security Guidelines for Vessels.

The Coast Guard issued NVIC 10–02 before the MTSA became effective. The MTSA required us to develop regulations for maritime security. We developed these regulations, including part 104, to align with SOLAS and the ISPS Code, not previously issued NVICs.

Two commenters asked for clarification on applicability for government vessels. One commenter stated that there should be some form of regulation that covers security on government vessels. One commenter opposed exempting government vessels from part 104 if the vessel is leased to a private organization for commercial purposes.

The MTSA exempts certain government-owned vessels from the requirement to prepare and submit Vessel Security Plans. However, if a government-owned vessel engages in commercial service or carries even a single passenger for hire, these vessels are subject to these regulations. For those certain government-owned vessels exempt from security plans by the MTSA, the COTP will continue to work to ensure that security measures appropriate for these vessels' operations are addressed in a manner similar to our current oversight of safety measures.

Two commenters asked whether the submission requirement for Vessel Security Plans applies to foreign flag vessels.

As outlined in § 104.115(c), foreign flag vessels carrying a valid ISSC do not have to submit a Vessel Security Plan to the Coast Guard. Owners and operators of foreign flag vessels not required to comply with SOLAS must either submit their plans to the Coast Guard for approval, or comply with an Alternative Security Program implemented by their flag administration that has been approved by the Coast Guard. Additionally, we are amending § 104.140(b) to clarify that vessels subject to SOLAS may not use an Alternative Security Program.

Three commenters recommended developing an International Maritime Organization (IMO) list of port facilities to help foreign shipowners identify U.S. facilities not in compliance with subchapter H. In a related comment, there was a request for the Coast Guard to maintain and publish a list of non-compliant facilities and ports because a COTP may impose one or more control and compliance measures on a domestic or foreign vessel that has called on a facility or port that is not in compliance.

We do not intend to publish a list of each individual facility that complies or does not comply with part 105. As discussed in the temporary interim rule (68 FR 39262) (part 101), our regulations align with the requirements of the ISPS Code, part A, section 16.5, by using the AMS Plan to satisfy our international obligations to communicate to IMO, as required by SOLAS Chapter XI–2, regulation 13.3, the locations within the U.S. that are covered by an approved port facility security plan. Any U.S. facility that receives vessels subject to SOLAS is required to comply with part 105.

Two commenters asked for specific exemptions for specific vessels from these final rules.

This request is beyond the scope of these final rules. If part 104 applies to a vessel, the vessel owner or operator may request a waiver under the provisions of § 104.130; however, the only exemptions to part 104 are found in § 104.110. Questions on applicability for specific vessels should be directed to the local COTP.

Twelve commenters questioned our compliance dates. One commenter stated that because the June 2004 compliance date might not be easily achieved, the Coast Guard should consider a ''phased in'' approach to implementation. Four commenters asked us to verify our compliance date expectations and asked if a facility can ''gain relief'' from these deadlines for good reasons.

The MTSA requires full compliance with these regulations 1 year after the publication of the temporary interim rules, which were published on July 1, 2003. Therefore, a ''phased in approach'' will not be used. While compliance dates are mandatory, a vessel or facility owner or operator could ''gain relief'' from making physical improvements, such as installing equipment or fencing, by addressing the intended improvements in the Vessel or Facility Security Plan and explaining the equivalent security measures that will be put into place until improvements have been made.

In order to clarify compliance dates for the rule, we are amending the dates of compliance in § 104.115(a) and (b), § 104.120(a), § 104.297(c), and § 104.410(a) to align with the MTSA and the ISPS Code compliance dates.

Seven commenters observed that the deadline for submitting Vessel Security Assessments and Vessel Security Plans for foreign vessels to the Coast Guard is 6 months sooner than the deadline in SOLAS. Three commenters asked that § 104.115(a) be revised for clarification of the submission requirements for owners and operators of foreign flag vessels.

Foreign flag vessels need not submit their Vessel Security Assessments or Vessel Security Plans to the Coast Guard for review or approval. We have revised §§ 104.115, 104.120(a)(4), and 104.410(a), to clarify that owners and operators of foreign flag vessels that meet the applicable requirements of SOLAS Chapter XI will not have to submit their assessments or plans to the Coast Guard for review or approval. These amendments also clarify that foreign vessels, which may not be subject to or operating under SOLAS, may meet these requirements through either submission to the Coast Guard or their own flag administration. Flag administrations may apply the new international security requirements to vessels other than those required to comply with SOLAS, consistent with paragraph 4.46 of part B of the ISPS Code and Resolution 7 from IMO's Diplomatic Conference on Maritime Security. Furthermore, some flag administrations not party to SOLAS may decide to apply SOLAS Chapter XI and the ISPS Code requirements to their vessels trading with the U.S. In these latter two cases-where foreign vessels not subject to SOLAS may nevertheless be required by the flag administration to comply with the requirements of SOLAS Chapter XI and the ISPS Code-the Coast Guard intends to work with the flag administration if they propose initiatives such as an Alternative Security Program. This will likely be done through bilateral or multilateral arrangements. When no approved Alternative Security Program or bilateral arrangement exists, foreign flag vessels not subject to SOLAS covered by 33 CFR part 104 must submit their Vessel Security Assessments and Vessel Security Plans to the Coast Guard for review and approval.

Three commenters stated they were concerned that any U.S. flag vessel on an international voyage after July 1, 2004, without a proper ISSC, and possessing only a letter from the Marine Safety Center stating that its ''Vessel Security Plan was under review'' would be detained by foreign Port State Control Authorities. The commenter further suggested that we establish a priority system to complete the plan reviews of those vessels engaging on international voyages first.

We recognize the position a U.S. flag vessel may be in if it does not have an approved Vessel Security Plan and ISSC issued to it by July 1, 2004. Vessel Security Plans must be submitted to the Coast Guard by December 31, 2003. We plan to complete the review and approval of the Vessel Security Plans as soon as possible to allow the owners or operators enough time to request an inspection, at least 30 days prior to the desired inspection date, from the Officer in Charge, Marine Inspection at the port where the vessel will be inspected to verify compliance. Following verification of compliance the Coast Guard will issue an ISSC as appropriate before the July 1, 2004, entry into force date. We urge vessel owners and operators to work closely with the Coast Guard since the MTSA mandates that no vessel subject to this part may operate in waters subject to the jurisdiction of the U.S. after July 1, 2004, without an approved Vessel Security Plan.

We received three comments on Recognized Security Organizations (RSOs). One commenter believed that any question of ''underperformance'' on the part of an RSO should be taken up with the flag state that has made the designation and should not, in the first instance, be sufficient justification for the application of control measures on a vessel that has been certified by the RSO in question. Another commenter recommended that the Coast Guard maximize national consistency and transparency with regard to the factors that are evaluated in the targeting matrix. One commenter supported the Coast Guard's plan to use Port State Control to ensure that Vessel Security Assessments, Plans, and ISSCs approved by designated RSOs comply with the requirements of SOLAS and the ISPS Code.

In conducting Port State Control, the Coast Guard will consider the ''underperformance'' of an RSO. However, a vessel's or foreign port facility's history of compliance will also be important factors in determining what actions are deemed appropriate by the Coast Guard to ensure that maritime security is preserved.

Seven commenters requested that reference to the ISPS Code, part B, be removed from § 104.105(c) because according to IMO guidance, part B must be considered when a vessel's ISSC is issued; therefore, the commenters believe our requirement is unnecessary. One commenter requested that we state what type of attestation is acceptable to demonstrate that an ISSC has taken into account the relevant provisions of part B.

We have amended §§ 104.105(c) and 104.120 to clarify that we are not requiring separate documentation for application of the ISPS Code, part B. Foreign flag vessels required to comply with SOLAS Chapter XI–2 and the ISPS Code are required only to have on board a valid ISSC issued in accordance with section 19 of part A of the ISPS Code. This includes ensuring that the Vessel Security Plan meets the requirements in SOLAS Chapter XI–2 and the ISPS Code, part A, having taken into account the relevant provisions of part B. The form of the ISSC is contained in Appendix 1 of the ISPS Code, part A. There is no separate requirement in our regulations to document compliance with part B, although we do encourage flag administrations and RSOs to provide such documentation to assist our Port State Control efforts and reduce the potential for vessel delays. Although optional, this documentation could be in the form of a letter retained on board the vessel, signed by an authorized representative of the flag administration or RSO that clearly states that the Vessel Security Plan applies the relevant provisions of part B. We intend to use part B as one of the tools to assess a foreign vessel's compliance with SOLAS Chapter XI–2 and the ISPS Code, part A. We amended § 104.400(b) to be consistent with changes made above to clearly state that owners and operators of foreign flag vessels do not need to submit Vessel Security Plans if they have on board a valid ISSC.

Eleven commenters addressed the reference to the ISPS Code, part B, in the regulations. Three commenters asked whether the Coast Guard would accept an ISSC as evidence that a vessel was in compliance with the relevant provisions in the ISPS Code, part B.

Three commenters commended the Coast Guard for accepting an ISSC as *prima facie* evidence that the ship's flag administration has completed its obligation. One of these commenters also urged the Coast Guard to continue in its effort to ensure that domestic regulations ''mesh'' with the ISPS code.

As stated in § 104.120(a)(4), the ISSC will be considered evidence that the vessel complies with the ISPS Code, part A, and has taken into account the relevant provisions of part B.

Two commenters suggested that we add sample text to part 104 that would provide guidance to flag-state administrations on how to document foreign flag vessel compliance with the relevant provisions of the ISPS Code.

We disagree with the commenters. The Coast Guard cannot dictate to a foreign flag state administration the format of documentation to use to demonstrate compliance with the ISPS Code.

Several commenters had questions or comments regarding relationship between the regulations and the ISPS Code. Three commenters asked us to specify the procedures or dates, under our rules, with which foreign vessels must comply and that are different from SOLAS or ISPS Code requirements. Three commenters stated that it is inappropriate for the temporary interim rule to refer to the provisions of the ISPS Code, part B, as ''requirements.'' One commenter stated that the acceptance of a foreign vessel's ISSC presumes responsibility and compliance by a regime that is designed to avoid responsibility and compliance and imparts a multi-lateral interpretation on a unilateral Congressional intent. The commenter went further to state that permitting flag administrations to follow their own compliance methods may lead to corruption due to fraudulent, criminal, and terrorist-related activity.

We are using the same cooperative arrangement that we have used with success in the safety realm by accepting SOLAS certificates documenting flag-state approval of foreign SOLAS Vessel Security Plans that comply with the comprehensive requirements of the ISPS Code. The consistency of the international and domestic security regimes, to the extent possible, was always a central part of the negotiations for the MTSA and the ISPS Code. In the MTSA, the Congress explicitly found that ''it is in the best interests of the U.S. to implement new international instruments that establish'' a maritime security system. We wholeheartedly agree and will exercise Port State Control to ensure that foreign flag vessels have approved plans and have, in fact, implemented adequate security standards. Port State Control will not be delegated to anyone. If vessels do not meet our security requirements, we have the power to prevent those vessels from entering the U.S., and we will not hesitate to use that power in appropriate cases. The Port State Control measures will include tracking the performance of all owners, operators, flag administrations, RSOs, charterers, and port facilities. Noncompliance will subject the vessel to a range of control and compliance measures, which could include denial of entry into port or significant delay. A vessel's or foreign port facility's history of compliance, or lack thereof, or security incidents involving a vessel or port facility will be important factors in determining what actions are deemed appropriate by the Coast Guard to ensure that maritime security is preserved. The Coast Guard's current Port State Control program has been highly effective in ensuring compliance with SOLAS safety requirements, and we believe that the incorporation of the ISPS Code requirements into this program is the most efficient and effective means to carry out our Port State Control responsibilities, enhance our ability to identify substandard vessels, ensure the security of our ports, and meet the Congressional intent of the MTSA.

After further review of parts 101 and 104 through 106, we have also amended §§ 101.120(b)(3), 104.120(a)(3), 105.120(c), and 106.115(c) to clarify that a vessel or facility that is participating in the Alternative Security Program must complete a vessel or facility specific security assessment report in accordance with the Alternative Security Program, and it must be readily available.

Three commenters asked that the Coast Guard clarify the meaning of ''scheduled inspection'' as indicated in § 104.120(b). One commenter suggested that Vessel Security Plans and related security documentation should be inspected at the annual Coast Guard documentation inspection and not at a separate inspection.

The Coast Guard conducts scheduled inspections during which time the Coast Guard requests and reviews documentation on board the vessel. In § 104.120(b), we require that the Vessel Security Plan and related security documentation be made available upon request to the Coast Guard during a scheduled inspection. A scheduled inspection is an inspection such as for the issuance of a Certificate of Inspection or an annual re-inspection for endorsement on a Certificate of Inspection. For uninspected vessels, we intend to check compliance with these regulations at a frequency that is similar to those existing uninspected vessel safety programs and in conjunction with other boardings.

One commenter requested that we clarify § 105.125, ''Noncompliance,'' to ''focus on only those areas of noncompliance that are the core building blocks of the facility security program'' stating that the section requires a ''self-report [of] every minor glitch in implementation.''

We did not intend for § 105.125 to require self-reporting for minor deviations from these regulations if they are corrected immediately. We have clarified §§ 104.125, 105.125, and 106.120 to make it clear that owners or operators are required to request permission from the Coast Guard to continue operations when temporarily unable to comply with the regulations.

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.

Two commenters asked us to amend § 104.130 regarding waivers for vessels in order to explicitly address ''vessel-to-vessel interfaces.''

Any vessel owner or operator may apply for a waiver of any requirement of part 104, including the vessel-to-vessel activity provisions, that the owner or operator considers unnecessary in light of the nature of the operating conditions of the vessel. We are not adding any explicit references to particular

requirements that may be waived because listing these requirements could be interpreted as the only requirements that could be eligible for a waiver.

Two commenters stated that the Master should be added as a party, in addition to the owner or operator, to comply with MARSEC Directives.

We believe that the ultimate responsibility for ensuring compliance with 33 CFR part 104 and MARSEC Directives belongs to the owner or operator. The Master is always accountable to the owner or operator as an employee, and is responsible for the safety and security of the vessel.

One commenter questioned the need of long-range tracking for foreign vessels. The commenter also stated that only flag states should have the right to track their vessels worldwide and that port states should have only the capability to track vessels that have indicated an intention to enter port.

We have not addressed long-range tracking in this final rule because it is beyond the scope of this regulation.

*Subpart B—Vessel Security Requirements*

This subpart describes the responsibilities of the vessel owner, operator, and personnel relative to vessel security. It includes requirements for training, drills, recordkeeping, and Declarations of Security. It identifies specific security measures, such as those for access control, cargo handling, monitoring, and particular classes of vessels.

Two commenters suggested that the Coast Guard should not regulate security measures but should establish security guidelines based on facility type, in essence creating a matrix with ''risk-levels'' and suggested measures for facility security.

We cannot establish only guidelines because the MTSA and SOLAS require us to issue regulations. We have provided performance-based, rather than prescriptive, requirements in these regulations to give owners or operators flexibility in developing security plans tailored to vessels' or facilities' unique operations.

One commenter asked who would be ensuring the integrity of security training and exercise programs.

Since the events of September 11, 2001, the Coast Guard has developed a directorate responsible for port, vessel, and facility security. This directorate oversees implementation and enforcement of the regulations found in parts 101 through 106. Additionally, owners and operators of vessels and facilities will be responsible for recordkeeping regarding training, drills, and exercises. The Coast Guard intends to review these records during periodic inspections.

We received two comments on the requirements in § 104.200 regarding vessel owners and operators, stating that the provisions in this section are overly burdensome and difficult to implement.

We recognize that the provisions of § 104.200 may be challenging for some vessel owners and operators to implement. We have drafted this section to allow for maximum flexibility while ensuring that we address those vessels and operations that may be involved in a transportation security incident. Effective communication and coordination procedures for company employees, vessel crew, and others with whom they interact are necessary elements of maritime security. We believe that the maritime community, in large measure, already practices these procedures in their current operations. The intent of this section is to clarify those areas of maritime security that we believe every vessel owner and operator must consider as part of their operations.

Three commenters asked what security measures would be appropriate when taking barges from line boats to harbor boats to a barge fleeting area.

We understand that there are many diverse operations involved in the movement of tugs and barges, especially along rivers. In a towing vessel's Vessel Security Assessment, these operations and multiple barge interface activities must be evaluated. Those operations that make a barge-tug interface vulnerable to a transportation security incident must be mitigated through security measures detailed in the Vessel Security Plan for both the barge and the towing vessel. Some Alternative Security Programs tailored to tug and barge activities are being developed and may be useful in meeting these security requirements.

Nineteen commenters were concerned about the rights of seafarers at facilities. One commenter stated that the direct and specific references to shore leave in the regulations conform exactly with his position and the widespread belief that shore leave is a fundamental right of a seaman. One commenter stated that coordinating mariner shore leave with facility operators is important and should be retained, stating that shore leave for ships' crews exists as a fundamental seafarers' right that can be denied only in compelling circumstances. The commenter also stated that chaplains should continue to have access to vessels, especially during periods of heightened security. Four commenters requested that the regulations require facilities to allow vessel personnel access to the facilities for shore leave, or other purposes, stating that shore leave is a basic human right and should not be left to the discretion of the terminal owner or operator. One commenter stated that seafarers are being denied shore leave as they cannot apply for visas in a timely manner and that seafarers who meet all legal requirements should be permitted to move to and from the vessel through the facility, subject to reasonable requirements in the Facility Security Plan. One commenter stated that it is the responsibility of the government to determine appropriate measures for seafarers to disembark. One commenter encouraged the government to expedite the issuance of visas for shore leave.

We agree that coordinating mariner shore leave and chaplains' access to vessels with facility operators is important and should be retained. Sections 104.200(b)(6) and 105.200(b)(7) require owners or operators of vessels and facilities to coordinate shore leave for vessel personnel in advance of a vessel's arrival. We have not mandated, however, that facilities allow access for shore leave because during periods of heightened security shore leave may not be in the best interest of the vessel personnel, the facility, or the public. Mandating such access could also infringe on private property rights; however, we strongly encourage facility owners and operators to maximize opportunities for mariner shore leave and access to the vessel through the facility by seafarer welfare organizations. The Coast Guard does not issue, nor can it expedite the issuing of, visas. Additionally, visas are a matter of immigration law and are beyond the scope of these rules. Finally, it should also be noted that the government has treaties of friendship, commerce, and navigation with several nations. These treaties provide that seafarers shall be allowed ashore by public authorities when they and the vessel on which they arrive in port meet the applicable requirements or conditions for entry. We have amended §§ 104.200(b) and 105.200(b) to include language that treaties of friendship, commerce, and navigation should be taken into account when coordinating access between facility and vessel owners and operators.

After reviewing § 104.205, we made non-substantive editorial changes to clarify that Masters contact the Coast Guard via the National Response Center (NRC).

Two commenters requested that we add a provision that fully addresses the ''qualified individual'' portion of the

MTSA by allowing a Company Security Officer, Vessel Security Officer, Master, or other individual to serve as the qualified individual.

The MTSA does not require a company to designate a person as a ''qualified individual.'' Our requirements for the Company Security Officer, Vessel Security Officer, and the Master embody the MTSA requirement that the security plan identify who has full authority to implement security actions within a company.

One commenter stated that the responsibilities of a Company Security Officer in § 104.210 are too burdensome, too prescriptive, and outside the ''realm'' of what is associated with normal maritime operations.

It is not outside the realm of normal maritime operations for a company to consider security and the company's role in minimizing risk. We recognize that the provisions of § 104.210 may be challenging to implement for some Company Security Officers. We drafted this section to maximize the flexibility of Company Security Officers by allowing them to delegate responsibilities so long as the security of the company's operations is not compromised. The intent of this section is to outline those responsibilities that we believe are necessary for all Company Security Officers to effectively implement the security measures contained in Vessel Security Plans.

Seven commenters requested clarification on the roles of Company Security Officers and Vessel Security Officers. One commenter asked if they may be the same individual, or if the Coast Guard intended to have a minimum of two security officers within each company. Two commenters requested that we amend § 104.215 to allow the Vessel Security Officer to be a member of the crew or a ''regular complement of the vessel,'' stating that this would provide additional flexibility in assigning Vessel Security Officer responsibilities to others in the vessel's industrial complement and would not require a specific notation of the Vessel Security Officer on the vessel's Certificate of Inspection.

Sections 104.210(a)(3) and 104.215(a)(1) do not preclude an owner or operator of a company that owns vessels from appointing the same individual as both the Company Security Officer and Vessel Security Officer. The Company Security Officer may also be the Vessel Security Officer, provided he or she is able to perform the duties and responsibilities required of both positions. Generally, this provision is for vessels operating on restricted routes in a single COTP zone and for unmanned vessels. Under § 104.215(a)(2), however, the Vessel Security Officer for manned vessels must be the Master or a member of the crew. While we are making amendments to § 104.215 to clarify security responsibilities for unmanned vessels, we are not amending this section to explicitly identify the personnel that can be designated as crew because we intended the term ''crew'' to be sufficiently broad and include those persons that constitute the ''regular complement of the vessel.'' A vessel's Certificate of Inspection is issued under Title 46 of the Code of Federal Regulations and delineates crew as the vessels' complement for the safe operation and navigation of the vessel. While 33 CFR chapter I, subchapter H focuses on security, the broader interpretation of ''crew'' includes individuals and crew necessary for the safe operation and navigation of the vessel as well as those ''persons in addition to the crew.'' Thus, a Certificate of Inspection need not be amended to include a reference to the Vessel Security Officer.

Nine commenters requested formal alternatives to Facility Security Officers, Company Security Officers, and Vessel Security Officers much like the requirements of the Oil Pollution Act of 1990, which allow for alternate qualified individuals. Parts 104, 105, and 106 provide flexibility for a Company, Vessel, or Facility Security Officer to assign security duties to other vessel or facility personnel under §§ 104.210(a)(4), 104.215(a)(5), 105.205(a)(3), and 106.310(a)(3). An owner or operator is also allowed to designate more than one Company, Vessel, or Facility Security Officer. Because Company, Vessel, or Facility Security Officer responsibilities are key to security implementation, vessel and facility owners and operators are encouraged to assign an alternate Company, Vessel, or Facility Security Officer to coordinate vessel or facility security in the absence of the primary Company, Vessel, or Facility Security Officer.

One commenter stated that allowing the Vessel Security Officer and Facility Security Officer to perform collateral non-security duties is not an adequate response to risk.

Security responsibilities for the Company, Vessel, and Facility Security Officers in parts 104, 105, and 106 may be assigned to a dedicated individual if the owners or operators believe that the responsibilities and duties are best served by a person with no other duties.

Two commenters requested amending § 104.210 regarding the duties of the Company Security Officer to include explicit consideration of vessel-to-vessel activities.

The responsibilities in § 104.210 are in addition to requirements specified elsewhere in part 104. Security duties relating to vessel-to-vessel activities are not specifically assigned to either the Company Security Officer or the Vessel Security Officer. Vessel-to-vessel activities are addressed in § 104.250(a), where the vessel owner or operator must ensure that there are measures for interfacing with facilities and other vessels at all MARSEC Levels. This provides the owner or operator of the vessel the flexibility to determine the most appropriate personnel to handle vessel-to-vessel security concerns for their specific operations.

One commenter stated that it is unreasonable and unenforceable to require the Company Security Officer of a foreign company, not headquartered in the U.S., to be knowledgeable of U.S. domestic regulations. Similarly, one commenter stated that it is unreasonable and unenforceable for us to require the Facility Security Officer to be trained in relevant international laws, codes, and recommendations.

We disagree. Foreign flag vessels are required to comply with these regulations, including the Company Security Officer requirements. However, we do provide that those vessels required to comply with SOLAS and the ISPS Code will comply with these regulations by having on board an ISSC and a Vessel Security Plan that meets the requirements of SOLAS XI–2 and the ISPS Code, part A, taking into account the relevant provisions of the ISPS Code, part

B. Paragraph 13.1.3 of part B expressly states that the Company Security Officer, among other security personnel, should have knowledge of ''relevant'' government legislation and regulations, which clearly is not limited solely to those of the flag state. Therefore, the requirement in the regulations reflects the international standard. Furthermore, we do prescribe additional domestic security requirements for some foreign vessels, such as cruise ships. Therefore, as a practical matter, Company Security Officers must be knowledgeable of these regulations to adequately perform their duties.

One commenter requested that the Company Security Officer be allowed to liaise with the Coast Guard at the District, Area, or Headquarters level rather than the local COTP.

We agree that effective communication may be established between the Company Security Officer

and one or more COTPs and that for some companies, effective communications with the Coast Guard may be at the District, Area, or Headquarters level; therefore, we are amending the definition of ''Company Security Officer'' in part 101 of this subchapter to remove the specific reference to the COTP.

We received three comments on the requirements of § 104.215 regarding the responsibilities of the Vessel Security Officer, stating that the provisions are too burdensome, too prescriptive, and outside the ''realm'' of what is associated with vessel crewmembers'' duties.

It is not outside the realm of a vessel crew's duties to consider security and their role in minimizing risk; we also recognize that not every crewmember would be able to meet the challenging Vessel Security Officer provisions of § 104.215. The intent of this section is to outline those responsibilities that we believe are necessary for all Vessel Security Officers to effectively implement the security measures contained in Vessel Security Plans. However, we have also constructed this section to maximize the flexibility of Vessel Security Officers by allowing them to assign security duties to other crewmembers so long as the security of the vessel's operations is not compromised. In this way, other crewmembers can assist the Vessel Security Officer and learn about security related duties. Additionally, we allow persons to display general knowledge, which they may acquire through training or through equivalent job experience.

We received seven comments on the training of security personnel. One commenter believes that the addition of a Vessel Security Officer course is ''just the latest of a long line of new requirements that are becoming an unreasonable burden on Merchant Marine Officers.'' One commenter requested that the Coast Guard develop materials, course books, and videos to be used by the industry to conduct security training. One commenter stated that the Coast Guard should develop a training standard consistent with the International Convention for Standards of Training, Certification and Watchkeeping for Seafarers, 1978 (STCW). Two commenters stated that formal security training for mariners, including Company Security Officers, become mandatory as soon as possible. One commenter urged DHS to establish an integrated training program for Facility Security Officers.

We have worked with several other Federal agencies and industry experts on training for the maritime industry and recognize that the cumulative requirements for a new mariner are extensive. Accordingly, we do not currently require formal training or classroom courses for Vessel Security Officers, and the standards being developed through section 109 of the MTSA are intended to be flexible and dynamic. We are working on competencies and model-course standards with the Maritime Administration (MARAD) through IMO. As discussed in the preamble to the temporary interim rule (68 FR 39253) (part 101), there are continuing international training initiatives that have proposed seven course frameworks that coincide with requirements under section 109 of the MTSA. The training competencies found in the ISPS Code and repeated domestically in the MTSA ensure a streamlined approach so mariners worldwide will face the same competencies. Completion of a single course will satisfy both national and international standards. As presently proposed, the training may take place in a formal classroom setting or may be conducted on board a vessel or in other suitable settings. It is the overarching goal of the international community to incorporate this security training into the requirements of STCW.

We received 19 comments regarding the Vessel Security Officer requirement for towing and unmanned vessels. Six commenters disagreed with the requirement for towing vessels to have a Vessel Security Officer, stating it is an impractical requirement for a two-man harbor-towing vessel and will not enhance security. Nine commenters asked that the regulatory language be revised to clarify whether the Master of the vessel may be appointed as the Vessel Security Officer. One commenter asked if the Vessel Security Officer can be designated by title instead of by name. Three commenters felt that the responsibilities of the Vessel Security Officer in § 104.215(a)(3) and (4) should fall to the Company Security Officer.

We have required Vessel Security Officers on towing vessels greater than 8 meters that engage in towing barges transporting hazardous or dangerous cargos, because it is imperative that the responsibility for security on these vessels be clearly established. Recognizing that some of these towing vessels will have a small crew complement, we have not prohibited the Master from being the Vessel Security Officer. We have clarified this by amending § 104.215(a)(2) to include a specific reference to the Master. Section 104.200 provides that the Vessel Security Officer can be designated by name or by title; therefore, we have not amended this section. The duties of the Vessel Security Officer ensure that a knowledgeable person is on board or is directly responsible for coordinating the implementation of the Vessel Security Plan. We did not intend to preclude a Company Security Officer from also serving as a Vessel Security Officer for a towing or unmanned vessel. We have amended § 104.210(a)(3) to clarify that the Company Security Officer may serve as a Vessel Security Officer, provided that he or she is able to perform the duties and responsibilities of a Company Security Officer.

Eight commenters disagreed with the requirement that a Vessel Security Officer must be a crewmember because it is contradictory for unmanned vessels.

We recognize that, for an unmanned vessel, the requirement in § 104.215 is not explicit as to whether the Vessel Security Officer must be a member of the crew. We have amended § 104.215 to clarify that a Vessel Security Officer for unmanned vessels must be an employee of the company rather than a member of the crew.

Two commenters requested that § 104.215(c)(4) and (5) be amended to include the Master of the vessel in all proposed changes to, or problems with, the Vessel Security Plan, stating that the present regulatory language implies that the Master of the vessel need not be included in important security actions regarding the vessel.

It is the responsibility of the Company Security Officer to ensure a Vessel Security Plan is modified whenever necessary. In order for the Vessel Security Officer to adequately perform required duties, it is imperative that the Vessel Security Officer be able to propose modifications to the Company Security Officer who is ultimately responsible for making the necessary amendments. Sections 104.215(c)(4) and (5) do not preclude the Master, or any other personnel with security duties, from being involved in modifications to the Vessel Security Plan. We anticipate that the Master and other personnel with security duties will most likely be involved in those modifications, and do not believe that these personnel must be given the specific responsibilities for reviewing potential changes to the Vessel Security Plan.

One commenter requested that we amend language in § 104.220(c) to read ''Identify suspicious activity that could indicate actions that may threaten security.''

To remain consistent with the ISPS Code requirements, we did not amend the language in § 104.220(c); however,

the intent of the wording in § 104.220(c) encompasses the concept of ''identifying suspicious activity that could indicate actions that may threaten security.''

Two commenters suggested that ferries be exempt from the ''while at sea'' clause in § 104.220(i) that requires company or vessel personnel responsible for security duties to have knowledge on how to test and calibrate security equipment and systems and maintain them, arguing that ferries are not oceangoing and, therefore, typically use a manufacturer's service representative to perform equipment testing and calibration while at the dock. In addition, one commenter requested clarification on whether a manufacturer's technical expert could be used to perform regularly planned maintenance at the ferry terminal.

We disagree with exempting ferry or facility security personnel from understanding how to test, calibrate, or maintain security equipment and systems. However, §§ 104.220 and 105.210 provide the company the flexibility to determine who should have an understanding of how to test, calibrate, and maintain security equipment and systems. By stating ''company and vessel personnel responsible for security duties must* * *, as appropriate,'' we have allowed a company to write a Vessel or Facility Security Plan that outlines responsibilities for security equipment and systems. If the company chooses to have company security personnel hold that responsibility, then vessel or facility security personnel would simply have to know how to contact the correct company security personnel and know how to implement interim measures as a result of equipment failures either at sea or in port. Sections 104.220 and 105.210 do not preclude a manufacturer's service representative from performing equipment maintenance, testing, and calibration.

Two commenters requested that ferries and their terminals be exempt from conducting physical screening, and therefore, should also be exempt from §§ 104.220(l) and 105.210(l), which require security personnel to know how to screen persons, personal effects, baggage, cargo, and vessel stores.

We disagree with exempting ferries and their terminals from the screening requirement and, therefore, will continue to require that certain security personnel understand the various methods that could be used to conduct physical screening. Because ferries certificated to carry more than 150 passengers and the terminals that serve them may be involved in a transportation security incident, it is imperative that security measures, such as access control, be implemented. Section 104.292 provides passenger vessels and ferries alternatives to identification checks and passenger screening. However, it does not provide alternatives to the requirements for cargo or vehicle screening. Thus, ferry security personnel assigned to screening duties should know the methods for physical screening. There is no corresponding alternative to § 104.292 for terminals serving ferries carrying more than 150 passengers; therefore, terminal security personnel assigned to screening duties should also know the methods for physical screening.

Forty-one commenters requested that §§ 104.225, 105.215, and 106.220 be either reworded or eliminated because the requirement to provide detailed security training to all contractors who work in a vessel or facility or to facility employees, even those with no security responsibilities such as a secretary or clerk, is impractical, if not impossible. The commenters stated that, unless a contractor has specific security duties, a contractor should only need to know how, when, and to whom to report anything unusual as well as how to react during an emergency. One commenter suggested adding a new section that listed specific training requirements for contractors and vendors.

The requirements in §§ 104.225, 105.215, and 106.220 are meant to be basic security and emergency procedure training requirements for all personnel working in a vessel or facility. In most cases, the requirement is similar to the basic safety training given to visitors to ensure that they do not enter areas that could be harmful. To reduce the burden of these general training requirements, we allowed vessel and facility owners and operators to recognize equivalent job experience in meeting this requirement. However, we believe contractors need basic security training as much as any other personnel working on the vessel or facility. Depending on the vessel or facility, providing basic security training (*e.g.*, how and when to report information, to whom to report unusual behaviors, how to react during an emergency) could be sufficient. To emphasize this, we have amended §§ 104.225, 105.215, and 106.220 to clarify that the owners or operators of vessels and facilities must determine what basic security training requirements are appropriate for their operations.

Two commenters requested that the word ''seasonal'' be deleted from § 104.230(b)(1) regarding requirements for drills, stating that the word ''seasonal'' is irrelevant for owners and operators of uninspected vessels.

We disagree that the word ''seasonal'' is irrelevant because 33 CFR subchapter H covers a diverse population of vessels and facilities, some of whose owners and operators consider their operations ''seasonal'' in nature. It is imperative that the subset of owners and operators of vessels who consider their operations ''seasonal,'' whether inspected or uninspected, know that they must comply with the requirements in § 104.230(b)(1).

Two commenters recommended that drills only be required for manned vessels in § 104.230 since it is not possible to conduct a drill on an unmanned barge.

We agree that the nature of unmanned barges precludes the intensive personnel drills required for testing the proficiency of vessel personnel. However, each vessel subject to part 104, whether manned or unmanned, is required to submit a Vessel Security Plan for approval that includes drill and exercise requirements. Under § 104.230(b)(2), this plan should include those drill requirements that are appropriate for the nature and scope of that vessel's activity and adequately prepare the Vessel Security Officer to respond to those threats the vessel is most likely to encounter.

Sixteen commenters stated that requirements in § 104.230(b)(4) are unreasonable for vessels with 2 to 3-person crews, stating that the requirements that a drill must be conducted if one of the personnel is replaced, which could be as often as daily, is burdensome. Additionally, three commenters suggested that crewmembers should receive credit for drills that they participate in while on board other similar vessels.

We agree that it could be difficult to conduct drills for companies that rotate crews frequently or have standing relief crews. We have, therefore, amended § 104.230 to allow companies that operate vessels of similar design not subject to SOLAS to develop training and drill schedules that are more appropriate to their operations while keeping the standard of 25 percent. For example, a company operating several similar towing vessels could hire new crewmembers, have them participate in a drill on board one towing vessel, then rotate those crewmembers to any of the similar vessels within that same company's fleet without needing to conduct another drill for the moved crewmembers. Finally, we added the word ''from'' between ''week'' and ''whenever'' in § 104.230(b)(4) for clarity.

One commenter agreed with our inclusion of tabletop exercises as a cost-effective means of exercising the security plan.

Three commenters requested that annual exercises be conducted every 3 years, arguing that current drills are already too burdensome.

We believe that exercising the Vessel Security Plan frequently is essential to ensure the plan is effectively implemented; therefore, we have kept the annual requirement for an exercise of the Vessel Security Plan. Recognizing that participation in exercises can be time consuming and challenging to coordinate, we have allowed and encourage vessel owners and operators to combine security exercises with other exercises as stated in § 104.230(c)(2)(iii).

Nine commenters stated that companies should be able to take credit toward fulfilling the drill and exercise requirements for actual incidents or threats, as under § 103.515.

We agree that, during an increased MARSEC Level, vessel and facility owners and operators may be able to take credit for implementing the higher security measures in their security plans. However, there are cases where a vessel or facility implementing a Vessel or Facility Security Plan may not attain the higher MARSEC Level or otherwise not be required to implement sufficient provisions of the plan to qualify as an exercise. Therefore, we have amended parts 104, 105, and 106 to allow an actual increase in MARSEC Level to be credited as a drill or an exercise if the increase in MARSEC Level meets certain parameters. In the case of OCS facilities, this type of credit must be approved by the Coast Guard in a manner similar to the provision found in § 103.515 for the AMS Plan requirements.

One commenter stated that the language in § 105.225, regarding recordkeeping, does not specify where the records should be kept. The commenter stated that it is presumed that such records may be kept off-site in a secure location accessible to the Facility Security Officer and other appropriate personnel. One commenter asked for clarification of sensitive security information because there is no suitable place for such information to be protected on board an unmanned vessel. One commenter recommended that records be kept onshore and not on board the vessel.

Sections 104.235(a) and 105.225(a) state that the records must be made available to the Coast Guard upon request, and §§ 104.235(c) and 105.225(c) state that the records must be protected from unauthorized access. Therefore, a facility or vessel owner or operator must ensure that records are kept safely and also are available for inspection by the Coast Guard upon request, but the records do not necessarily have to be kept at the facility or on board the vessel.

Seven commenters stated that security records for harbor boats should be readily available but should not be maintained on the vessel for the security of those records.

We agree, and in § 104.235(a), we state that the Vessel Security Officer must keep records and make them available to the Coast Guard upon request. For vessels that make only domestic voyages, with the exception of Declarations of Security, these records may be kept somewhere other than on board the vessel, so long as they can be made available to the Coast Guard expeditiously upon request. For vessels subject to SOLAS, the ISPS Code, part A, section 10 requires records to be kept on board.

Five commenters stated that recordkeeping requirements should be limited to manned vessels. One commenter recommended that the Company Security Officer maintain and update all information for unmanned vessel security.

We disagree with the commenters. The regulations allow for a Vessel Security Officer to be a company representative for unmanned vessels and to be directly responsible for executing the recordkeeping requirements as specified in § 104.235. The requirements do not preclude the Vessel Security Officer from performing other duties within the organization, such as the Vessel Security Officer for unmanned vessels, provided he or she is able to perform the duties and responsibilities required of the Company Security Officer. We agree that the nature of operations for an unmanned barge makes recordkeeping different from that on a manned vessel; however, each vessel subject to part 104, whether manned or unmanned, must include recordkeeping to ensure compliance. The regulations do not preclude the Company Security Officer from being assigned the recordkeeping duties for unmanned vessels.

Two commenters recommended that a sentence be added to the end of § 105.225(b)(1) that reads: ''Short domain awareness and other orientation-type training that may be given to contractor and other personnel temporarily at the facility and not involved in security functions need not be recorded.'' The commenters stated that this change would eliminate the unnecessary recordkeeping for this general ''domain awareness'' training.

We agree that the recordkeeping requirements in § 105.225 for training are broad and may capture training that, while necessary, does not need to be formally recorded. Therefore, we have amended the requirements in § 105.225(b)(1) to only record training held to meet § 105.210. We have also made corresponding changes to §§ 104.235(b)(1) and 106.230(b)(1).

Twelve commenters inquired about the recordkeeping requirements for Declarations of Security. One commenter asked how long Declarations of Security must be kept. Three commenters suggested the retention for Declarations of Security should align with the Declarations of Inspection requirement of 30 days. Two commenters asked how the Coast Guard would enforce the requirement to maintain the last 10 Declarations of Security when a vessel may not yet have acquired 10 Declarations of Security.

As specified under § 104.235(b)(7), manned vessels must keep on board the vessel a copy of the last 10 Declarations of Security and a copy of each continuing Declaration of Security for at least 90 days after the end of its effective period. We require both vessels and facilities to retain Declarations of Security after they expire. We require vessels to retain Declarations of Security for their last 10 port visits. In order to roughly align the facility's retention requirement, as closely as possible, with the vessel's retention requirement, we estimated the average voyage of an ocean-going vessel. Doing this, we determined that a facility's 90-day retention period would more closely align with the vessel's 10-port visit retention period rather than the 30-day period used for Declarations of Inspection. We recognize that many factors, such as not being within U.S. waters during MARSEC Levels 2 and 3, may delay a vessel's ability to accumulate 10 Declarations of Security. If a vessel has on board fewer than the number of Declarations of Security required in § 104.235(b)(7), we will accept this vessel as meeting the intent of the section so long as it can be verified that the vessel was not required to complete more than the number of Declarations of Security kept on board.

One commenter stated that the Company Security Officer rather than the Vessel Security Officer should certify the certified letter required by § 104.235(b)(8), which states the date the annual audit of the Vessel Security Plan was completed. The commenter stated that this would focus the

section's security and administrative responsibilities at a single level.

We disagree with the recommendation to substitute the Company Security Officer for the Vessel Security Officer in § 104.235(b)(8) because that section generally places recordkeeping requirements on the Vessel Security Officer. However, we have amended the section to allow either the Vessel Security Officer or the Company Security Officer to certify the annual audit letter because this will align better with § 104.415(b), which allows either the Company Security Officer or Vessel Security Officer to ensure the performance of the annual audit.

Three commenters stated that the record of the annual audit of the Vessel Security Plan should be certified and kept by the Company Security Officer for barges and towing vessels, not the Vessel Security Officer.

In § 104.235(b)(8), we require an annual audit letter to be kept by the Vessel Security Officer. The annual audit certifies that the Vessel Security Plan continues to meet the applicable requirements of this part. Therefore, it is appropriate that the Vessel Security Officer keep the annual audit letter with the Vessel Security Plan.

One commenter asked if foreign vessels must have the Vessel Security Assessment on board.

If the vessel is issued an ISSC by its flag state attesting to its compliance with the ISPS Code, we will not require the vessel to have a Vessel Security Assessment on board. We will ensure that the vessel is implementing an effective Vessel Security Plan, which must address identified vulnerabilities, through an aggressive Port State Control program.

We received 28 comments regarding communication of changes in the MARSEC Levels. Most commenters were concerned about the Coast Guard's capability to communicate timely changes in MARSEC Levels to facilities and vessels. Some stressed the importance of MARSEC Level information reaching each port area in the COTP's zone and the entire maritime industry. Some stated that local Broadcast Notice to Mariners and MARSEC Directives are flawed methods of communication and stated that the only acceptable means to communicate changes in MARSEC Levels, from a timing standpoint, are via e-mail, phone, or fax as established by each COTP.

MARSEC Level changes are generally issued at the Commandant level and each Marine Safety Office (MSO) will be able to disseminate them to vessel and facility owners or operators, or their designees, by various means. Communication of MARSEC Levels will be done in the most expeditious means available, given the characteristics of the port and its operations. These means will be outlined in the AMS Plan and exercised to ensure vessel and facility owners and operators, or their designees, are able to quickly communicate with us and vice-versa. Because MARSEC Directives will not be as expeditiously communicated as other COTP Orders and are not meant to communicate changes in MARSEC Levels, we have amended § 101.300 to remove the reference to MARSEC Directives.

Two commenters requested that § 104.240(a) and (b)(1) be amended to specify that vessels must implement appropriate security measures before interfacing with facilities that are not located in a port.

We agree that the vessel owner or operator, once notified of a change in MARSEC Level, must implement appropriate security measures before interfacing with a facility that is not located in a port area. Facilities covered under part 105 will be within a port; facilities located on the Outer Continental Shelf, however, may not be included in a port. These OCS facilities should have similar security provisions to ports to ensure security. Therefore, we are amending § 104.240 to ensure that the vessel owner or operator is required to implement appropriate security measures in accordance with its Vessel Security Plan prior to interfacing with an OCS facility.

One commenter said that only manned vessels are capable of calling to verify attainment of increased MARSEC Levels and recommended that the Facility Security Officer be required to report attainment for unmanned barges moored at the facility. One commenter asked for clarification of § 104.240(b)(2) because facility and barge fleets have control of unmanned vessels moored at their facilities.

We disagree with the commenter. The regulations allow for a Vessel Security Officer to be a company representative for unmanned vessels, who may be designated by the owner or operator to report on the attainment of increased MARSEC Levels to the appropriate COTP, as specified in § 104.240. Any vessel, manned or unmanned, must be under the cognizance of a Vessel Security Officer or a Company Security Officer to ensure security measures are properly implemented.

Seven commenters stated that although facility or vessel personnel need to understand the current MARSEC Level and have a heightened state of awareness, in most cases, the specifics of the threat should not be disclosed.

It is necessary for the vessel or facility personnel to know about threats to the vessel or facility because this helps to focus their attention on specific attempts or types of threats to the vessel or facility. To balance this need with sensitive security concerns, §§ 104.240(c) and 105.230(c) give the owners or operators discretion in deciding how much specific information needs to be disclosed to facility or vessel personnel.

One commenter stated that the requirement in § 104.240(c) to brief all vessel personnel of identified threats at MARSEC Level 2 is unattainable and pointed out that implementing MARSEC Level 2 does not require an identified threat.

The intent of the requirement is to disclose as much information as is available and appropriate to vessel personnel to mitigate risk even if a threat is not identified. If there is no identified threat, the Vessel Security Officer is still required to brief all vessel personnel, emphasizing reporting procedures and the need for increased vigilance.

One commenter stated that requirements in § 104.240 regarding MARSEC Level 3 requirements for towing or moving vessels, waterborne security patrols, armed security personnel, and screening vessels for dangerous substances and devices should be applicable to cruise and other oceangoing vessels, but not to ferries.

We disagree that ferries should be exempt from the requirements of § 104.240. Our risk assessment showed that vessels with frequent schedules carrying over 150 passengers may be involved in a transportation security incident. When a transportation security incident is probable or imminent, therefore, § 104.240(e) allows the Coast Guard to require vessels, including ferries, to arrange for waterborne security patrols, armed security personnel, and vessel screening, as appropriate, to mitigate threat. The Coast Guard, in accordance with the AMS Plan, MARSEC Directive, or other COTP order, will communicate additional security measures deemed necessary.

Thirty-three commenters stated that the public lacks either the authority or the expertise for implementing the security measures for MARSEC Level 3, which include armed patrols, waterborne security, and underwater screening.

We disagree and believe that owners and operators have the authority to implement the identified security measures. For example, it is well settled under the law of every State that an employer may maintain private security guards or private security police to protect his or her property. The regulations do not require owners or operators to undertake law enforcement action, but rather to implement security measures consistent with their longstanding responsibility to ensure the security of their vessels and facilities, as specifically prescribed by 33 CFR 6.16–3 and 33 CFR 6.19–1, by: Deterring transportation security incidents; detecting an actual or a threatened transportation security incident for reporting to appropriate authorities; and, as authorized by the relevant jurisdiction, defending themselves and others against attack. It is also important to note that the security measures identified by these commenters, while listed in §§ 104.240(e) and 105.230(e), are not exclusive and only relate to MARSEC Level 3 implementation. In many instances, the owner or operator may decide to implement these security measures through qualified contractors or third parties who can provide any expertise that is lacking within the owner's or operator's own organization and who also have the required authority.

Four commenters stated that enforcing security on U.S. waterways is an inherently governmental function, not the responsibility of the maritime industry; therefore, the commenters do not want the crewmembers of foreign flag vessels to perform waterside security.

The intent of these regulations is not to mandate the use of crewmembers to perform waterside security, although that is an option. Those vessel owners and operators choosing to implement waterside security to meet the requirement of § 104.265(f) to ensure access control through additional measures during MARSEC Level 2 and, to enhance the security of the vessel during MARSEC Level 3, may choose to enter into agreements with the facility owner or operator, private security firms, or other parties to enhance the security of the vessel.

We received two comments addressing the affects of MARSEC Level changes on the STCW and International Labor Organization (ILO) standards. One commenter asked for confirmation that implementing MARSEC Level 2 ''automatically exempts vessels from the STCW and ILO work hour and rest requirements.'' One commenter stated disappointment that the regulations did not address the need for increased manning at MARSEC Level 3 to ensure that personnel can perform additional duties and comply with STCW mandated rest periods.

Vessel owners and operators are not exempt from any existing work hour and rest requirements when implementing these security requirements at MARSEC Level 2 or 3. The Vessel Security Plan must address how the security measures will be implemented at each MARSEC Level. Manning concerns must be considered during the Vessel Security Plan development and addressed during the plan's implementation.

One commenter asked the Coast Guard to provide guidance for operations at MARSEC Level 3 for vessels arriving from international voyages on: notification procedures, specific organizations able to provide armed security guards, and organizations able to provide underwater monitoring.

The Notice of Arrival requirements are contained in 33 CFR part 160. We encourage vessel owners and operators to contact their shipping agents in the COTP zones in which they operate to obtain information on firms and organizations that provide security services.

One commenter asked how, in accordance with § 104.240(d), the COTP will communicate permission to a vessel to enter the port if the vessel cannot implement its Vessel Security Plan.

The COTP can use a number of means to communicate to a vessel permission or denial to enter the port, such as issuing a COTP order denying entry or establishing conditions upon which the vessel may enter the port. Presently, communications to a vessel occur before entry to the port regarding required construction, safety, and equipment regulations. These communications occur through agents by satellite phone, fax, email, cellular phone, or radio communications.

We received nine comments questioning our use of the words ''continuous'' or ''continuously'' in the regulations. Four commenters requested that we amend language in § 104.245(b) by replacing the word ''continuous'' with the word ''continual,'' stating that ''continuous'' implies that there must be constant and uninterrupted communications. One commenter requested that we amend language in § 104.285(a)(1) by replacing the word ''continuously'' with the word ''continually,'' stating that ''continuously'' implies that there must be constant and uninterrupted application of the security measure. One commenter requested that we amend language in § 106.275 to replace the word ''continuously'' with the word ''frequently.'' One commenter recommended that instead of using the word ''continuously'' in § 105.275, the Coast Guard revise the definition of monitor to mean a ''systematic process for providing surveillance for a facility.'' One commenter stated that the continuous monitoring requirements in § 106.275 place a significant burden on the owners and operators of OCS facilities because increased staff levels would be necessary to keep watch not only in the facility, but also in the surrounding area.

We did not amend the language in §§ 104.245(b) 105.235(b), or 106.240(b) because the sections require that communications systems and procedures must allow for ''effective and continuous communications.'' This means that vessel owners or operators must always be able to communicate, not that they must always be communicating. Similarly, §§ 104.285, 105.275, and 106.275, as a general requirement, require vessel and facility owners or operators to have the capability to ''continuously monitor.'' This means that vessel and facility owners or operators must always be able to monitor. We have amended §§ 104.285(b)(4) and 106.275(b)(4) to use the word ''continuously'' instead of ''continually'' to be consistent with § 105.275(b)(1). This general requirement is further refined in §§ 104.285, 105.275,and 106.275, in that the Vessel and Facility Security Plans must detail the measures sufficient to meet the monitoring requirements at the three MARSEC Levels.

Three commenters disagreed with the requirement to have a security alert system on a river harbor towing vessel because it would serve no useful purpose.

We have not required a security alert system for towing vessels unless they are also subject to SOLAS. In § 101.310 we state that a security alert system may be a useful addition to certain operations and could be used to meet some of the communications requirements in subchapter H; however, we did not mandate its use for all vessels.

Two commenters suggested that the Coast Guard should be responsible for facilitating communications between vessels and facilities.

We believe that it is the Coast Guard's role to ensure that vessels and facilities have the proper procedures and equipment for communicating with

each other. The Coast Guard does have communication responsibilities, as found in § 101.300. It is imperative, however, that vessels and facilities communicate with each other in order to effectively coordinate the implementation of security measures. Thus, we have placed this requirement on the owner or operator, not the Coast Guard. The Coast Guard will be inspecting facilities and vessels to ensure this communication is accomplished.

We received 14 comments about the length of the effective period of a continuing Declaration of Security for each MARSEC Level. Five commenters stated that there is little need to renew a Declaration of Security every 90 days and that it should instead be part of an annual review of the Vessel Security Plan. Three commenters stated that the effective period of MARSEC Level 1 should not exceed 180 days while the effective period for MARSEC Level 2 should not exceed 90 days. One commenter noted that a vessel may execute a continuing Declaration of Security and assumed that this means that a Declaration of Security for a regular operating public transit system is good for the duration of the service route. Three commenters recommended that the effective period for a Declaration of Security be either 90 days or the term for which a vessel's service to an OCS facility is contracted, whichever is greater. Two commenters recommended allowing ferry service operators and facility operators to enact pre-executed MARSEC Level 2 condition agreements rather than initiating a new Declaration of Security at every MARSEC Level change.

We disagree with these comments and believe that continuing Declaration of Security agreements between vessel and facility owners and operators should be periodically reviewed to respond to the frequent changes in operations, personnel, and other conditions. We believe that the Declaration of Security ensures essential security-related coordination and communication among vessels and facilities. Renewing a continuing Declaration of Security agreement requires only a brief interaction between vessel and facility owners and operators to review the essential elements of the agreement. Additionally, at a heightened MARSEC Level, that threat must be assessed and a new Declaration of Security must be completed. Less frequent review, such as during an annual or biannual review of the Vessel Security Plan, does not provide adequate oversight of the Declaration of Security agreement to ensure all parties are aware of their security responsibilities.

Five commenters requested that § 104.255(c) and (d) be amended so that a Declaration of Security need not be exchanged when conditions (*e.g.*, adverse weather) would preclude the exchange of the Declaration of Security.

We are not amending § 104.255(c) and (d) because as stated in § 104.205(b), if, in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the vessel arises during its operations, the Master may give precedence to measures intended to maintain the safety of the vessel and take such temporary security measures as deemed best under all circumstances. Therefore, if the Declaration of Security between a vessel and facility could not be safely exchanged, the Master would not need to exchange the Declaration of Security before the interface. However, under § 104.205(b)(1), (b)(2), and (b)(3), the Master would have to inform the nearest COTP of the delay in exchanging the Declaration of Security, meet alternative security measures considered commensurate with the prevailing MARSEC Level, and ensure that the COTP was satisfied with the ultimate resolution. In reviewing this provision, we realized that a similar provision to balance safety and security was not included in parts 105 or 106. We have amended these parts to give the owners or operators of facilities the responsibility of resolving conflicts between safety and security.

Five commenters asked whether a company could have an agreement with a facility that outlines the responsibilities of all the company's vessels instead of a separate Declaration of Security for each vessel. The commenters stated that this would make the Declaration of Security more manageable for companies, vessels, and facilities that frequently interface with each other. One commenter raised a similar concern regarding barges and tugs conducting bunkering operations. One commenter suggested that Declarations of Security not be required when the vessels and ''their docking facilities'' share a common owner.

As stated in §§ 104.255(e), 105.245(e), and 106.250(e), at MARSEC Levels 1 and 2, owners or operators may establish continuing Declaration of Security procedures for vessels and facilities that frequently interface with each other. These sections do not preclude owners and operators from developing Declaration of Security procedures that could apply to vessels and facilities that frequently interface. However, as stated in §§ 104.255(c) and (d), 105.245(d), and 106.250(d), at MARSEC Level 3, all vessels and facilities required to comply with parts 104, 105, and 106 must enact a Declaration of Security agreement each time they interface. We believe that, even when under common ownership, vessels and facilities must coordinate security measures at higher MARSEC Levels and therefore should execute Declarations of Security. For MARSEC Level 1, only cruise ships and vessels carrying Certain Dangerous Cargoes (CDC) in bulk, and facilities that receive them, even when under common ownership, are required to complete a Declaration of Security each time they interface.

Three commenters suggested that the regulations should require that the Vessel Security Officer and Facility Security Officer have verified-via email, phone, or other suitable means prior to the vessel's arrival in the port-that the provisions of the Declaration of Security remain valid.

We disagree that there is a need to specify the means of communicating between the Vessel Security Officer and the Facility Security Officer about the provisions of the Declaration of Security. To maintain flexibility, the regulations neither preclude nor mandate a specific means to use when discussing a Declaration of Security.

Eight commenters stated that there is significant confusion regarding the requirements to complete Declarations of Security, especially when dealing with unmanned barges. One commenter asked if a Declaration of Security is required when an unmanned barge is ''being dropped'' at a facility or when ''changing tows.''

We agree with the commenter and are amending §§ 104.255(c) and (d) and 106.250(d) to clarify that unmanned barges are not required to complete a Declaration of Security at any MARSEC Level. This aligns these requirements with those of § 105.245(d). At MARSEC Levels 2 and 3, a Declaration of Security must be completed whenever a manned vessel that must comply with this part is moored to a facility or for the duration of any vessel-to-vessel activity.

Three commenters asked when the Coast Guard would communicate standards for U.S. flag vessels and facilities as to the timing and format of a Declaration of Security. One commenter requested information about how Declaration of Security requirements will be communicated to and coordinated with vessels that do not regularly call on U.S. ports and specific facilities.

As specified in § 101.505, the format of a Declaration of Security is described

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

and operators are required to give particular consideration to the convenience, comfort, and personal privacy of vessel personnel. Taken as a whole, these rules strike the proper balance between implementing the MTSA's provisions for deterring transportation security incidents and preserving constitutional rights to privacy, travel, and association.

One commenter recommended that the ''means of access'' listed in § 104.265(b)(1) should only include traditional vessel access areas.

Each vessel must perform a Vessel Security Assessment, as required by § 104.305, to identify those areas that provide a means of access to the vessel. The list of means of access provided in § 104.265(b)(1) is not intended to be an all-inclusive or minimum list for each individual vessel.

One commenter suggested we remove § 104.265(c)(6), which allows certain, long-term, frequent vendor representatives to be treated more as employees than as visitors.

We disagree with the commenter. This language is found in the ISPS Code and provides additional flexibility when dealing with these frequent representatives.

One commenter asked if the Coast Guard would issue guidelines on screening.

The Coast Guard intends to coordinate with the Transportation Security Administration (TSA) and the Bureau of Customs and Border Protection (BCBP) in publishing guidance on screening to ensure that such guidance is consistent with intermodal policies and standards of TSA, and the standards and programs of BCBP for the screening of international passengers and cargo. Additionally, TSA is developing a list of items prohibited from being carried on board passenger vessels.

One commenter recommended removing the provision that mandated screening of persons, baggage, and vehicles at MARSEC Level 1. The same commenter also recommended removing the provision for designations of a secure area on board the vessel for the purposes of screening ''baggage (including carry on items), personal effects, vehicles, and the vehicle's contents.''

We disagree with the commenter. We believe that screening of persons, their personal effects, and vehicles are necessary at all MARSEC Levels to minimize the risk of a transportation security incident. However, while we mandate that all vessels must implement screening procedures, we provide the flexibility for those vessels to determine what those screening procedures should be, taking into account the type of vessel and the geographical region where that vessel is operating. Additionally, the intent of the regulations is that the secure area used to conduct the screening of baggage or personal effects could be the same location where the screening of persons entering the vessel takes place. Because we have kept the screening requirements in these final rules, we have also retained the provisions for designating a secure area on board the vessel or in liaison with the facility for conducting inspections and screening.

We received two comments on vehicle searches. One commenter stated that vehicle screenings prior to boarding vessels ''are not warranted.'' One commenter suggested that the government is responsible for vehicle inspections and searches.

We disagree. Vehicles may be used to cause a transportation security incident. Therefore, the screening of vehicles is warranted.

We received requests from other Federal agencies to clarify that government-owned vehicles on official business should not be subject to search. We agree and are amending § 104.265(e)(1) to exempt government-owned vehicles on official business from screening or inspection. This does not exempt government personnel from presenting identification credentials on demand for entry onto vessels or facilities.

One commenter suggested using bomb-sniffing dogs to scan all vehicles in a ferry lot prior to boarding a ferry, along with ''uniformed troopers'' who remain visible for the trip.

Section 104.265 gives ferry owners and operators the flexibility to implement those security measures that meet the given performance standards. Owners and operators of ferry terminals and vessels may submit security plans that include security measures such as bomb-sniffing dogs and uniformed security guards to meet the performance standards in security plans.

Three commenters stated that they want to be able to lawfully carry firearms on ferries and do not want to check their firearms on a short ferry trip.

While the regulations require vessel owners and operators to deter the introduction of dangerous substances and devices, in accordance with § 104.265, the regulations do not mandate the checking of lawfully carried firearms. Our regulations are flexible to handle daily operations and allow the owners and operators to develop appropriate procedures that ensure the security of its passenger or commercial activities. All security plans will be reviewed by the Coast Guard to ensure compliance with access control regulations.

Three commenters stated that many of the requirements of § 104.265, Security measures for access control, should not apply to unmanned vessels because there is no person on board the vessel at most times.

We disagree. The owner or operator must ensure the implementation of security measures to control access because unmanned barges directly regulated under this subchapter may be involved in a transportation security incident. As provided in § 104.215(a)(4), the Vessel Security Officer of an unmanned barge must coordinate with the Vessel Security Officer of any towing vessel and Facility Security Officer of any facility to ensure the implementation of security measures for the unmanned barge. We have amended § 105.200 to clarify the facility owner's or operator's responsibility for the implementation of security measures for unattended or unmanned vessels while moored at a facility.

One commenter asked if there is a difference between the terms ''screening'' and ''inspection'' as used in § 104.265(e)(2), requiring conspicuously posted signs.

In 33 CFR subchapter H, the terms ''screening'' and ''inspection'' fully reflect the types of examinations that may be conducted under §§ 104.265, 105.255, and 106.260. Therefore, both terms are included to maximize clarity.

We received 10 comments regarding signage and posting of signs. Ten commenters stated that posting new signs required in § 104.265(e)(2), on board unmanned barges that describe the security measures in place is unnecessary because existing signs indicate that visitors are not permitted on board. One commenter stated that the requirements in § 105.255(e)(2) regarding signage are too prescriptive and believed that facilities should be allowed to post signs as they deem necessary and not attract additional attention.

We disagree with the comment and believe that signs, appropriately posted, serve as a deterrent against unauthorized entry and provide awareness for facility security personnel. Although signage is primarily aimed at manned vessels, we extended this to all vessels because all vessels may on occasion be boarded by persons whose entry would subject them to possible screening. If existing signs accomplish this, the owner or operator is in compliance with the regulation.

One commenter stated that the prohibitions regarding vessel personnel screening by other vessel personnel should apply at all MARSEC Levels.

The intent of § 104.265(e)(9) is to require the owner or operator of a vessel to ensure that crewmembers do not engage in screening other crewmembers. We have amended the paragraph for clarity.

Sixteen commenters voiced concern that the regulations may require that security personnel and crewmembers be armed. Six commenters suggested § 104.265(e)(15) be amended to read: ''Response to the presence of unauthorized persons on board,'' stating that the current regulatory text implies that security personnel must be armed, which poses unacceptable risks to the vessel and its crew. Five commenters suggested revising §§ 104.290(a)(1) and (2) unless it is meant that crewmembers be armed as first responders during an attack. Three commenters stated that facility employee responsibilities should ''not include meeting force with force.'' Three commenters suggested that we amend § 104.290(a)(1) to revise ''Prohibiting'' to read ''Deter to the best of their ability'' and § 104.290(a)(2) to revise ''Deny'' to read ''Denying access to the best of their ability.''

The regulatory language in § 104.265(e)(15) does not require that vessel personnel be armed in order to repel unauthorized personnel onboard, although it is an option. The requirement to respond to unauthorized personnel onboard a vessel does not necessarily require security personnel to repel unauthorized boarders, but rather to have in place measures that will detect and deter persons from gaining unauthorized access to the vessel or facility. If unauthorized access is attempted or gained at a vessel or facility, then the Vessel Security Plan or Facility Security Plan must describe the security measures to address such an incident, including measures for contacting the appropriate authorities and preventing the unauthorized boarder from gaining access to restricted areas. We are not requiring the owner or operator to put any personnel in ''harm's way,'' (*i.e.*, by mandating using deadly force to confront deadly force). We have not changed § 104.290 as suggested by the commenter because we believe these suggested changes would erode the level of security to be achieved by the regulations. Owners and operators may find guidance in the IMO's Circular titled ''Piracy and Armed Robbery, Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships,'' MSC/Cir.623/Rev.3, to be a useful reference in this regard. We are amending § 104.265(b) to include a verb in the sentence for clarity. We are also mirroring this clarification in §§ 105.255(b) and 106.260(b).

Nine commenters were concerned about the designation of restricted areas. Six commenters requested that the Coast Guard clarify the wording in §§ 104.270(b) and 105.260(b) that states ''Restricted areas must include, as appropriate:'' because it is contradictory to impose a requirement with the word ''must,'' while offering the flexibility by stating ''as appropriate.'' One commenter stated that the provision that allows owners or operators to designate their entire facility as a restricted area could result in areas being designated as restricted without any legitimate security reason.

We believe that the current wording of §§ 104.270(b), 105.260(b), and 106.265(b) is acceptable. While the word ''must'' requires owners or operators to designate restricted areas, the word ''appropriate'' allows flexibility for owners or operators to restrict areas that are significant to their operations. The regulations provide for the entire facility to be designated as a restricted area, whereby a facility owner or operator would then be required to provide appropriate security measures to prevent unauthorized access into the entire facility.

One commenter stated that a ''ventilation and air-conditioning system'' as stated in § 104.270(b)(3) cannot be marked as a restricted area, and requested it be changed to read ''ventilation and air-conditioning system control spaces.''

Section 104.270(b)(3) aligns with the wording of the ISPS Code. The term ''spaces'' modifies the terms ''ventilation and air-conditioning system'' in the requirement. The intent of this requirement in the ISPS Code development was to align with various other control space definitions such as those found in SOLAS, Chapter II–2. Therefore, we have not revised the text in § 104.270 but intend to address control spaces and restricted area designations in plan review guidance.

One commenter stated that it is impractical and unsafe to lock all access ways to vessel crew accommodations, which are restricted areas, noting that the more doors that are locked in ''normal passageways'' the less safe the vessel becomes.

Section 104.270(d) provides a non-exhaustive list of security measures that an owner or operator may use to prevent unauthorized access to restricted areas. Only one of these measures is locking or securing access points to restricted areas. Other methods include monitoring, using guards, or using automatic intrusion detection. The owner or operator may also use other measures to prevent unauthorized access. Finally, we recognize the potential competition between maximizing safety and maximizing security and in § 104.205(b), state, that ''If * * * a conflict between any safety and security requirements applicable to the vessel arises during its operations, the Master may give precedence to measures intended to maintain the safety of the vessel, and take such temporary security measures as seem best under all circumstances.'' However, this provision does not circumvent overall security of vessels because the section also requires, in § 104.205(b)(3), that the owner or operator ensure the conflict is permanently resolved to the satisfaction of the Coast Guard.

Fourteen commenters stated that the requirements in § 104.275 regarding cargo handling are overly burdensome and difficult to implement. One commenter suggested that the regulations ensure that empty containers be opened and inspected. Three commenters stated it is not possible for a vessel owner or operator to ensure that cargo is not tampered with prior to being loaded, to identify cargo being brought on board, or to check cargo for dangerous substances. One commenter stated that imports should be screened at the loading port, not once they were in the U.S. and that the U.S. focus should be on knowing with whom vessel owners and operators are doing business. One commenter urged that the final rule clarify whether coordinating security measures with the shipper or other responsible party is mandatory. One commenter stated that checking cargo for dangerous substances or devices is a governmental function. Three commenters stated that the requirement in § 105.265(a)(9) to maintain a continuous inventory of all dangerous goods and hazardous substances passing through the facility is unnecessarily burdensome and should be deleted.

We recognize that screening for dangerous substances and devices is a complex and technically difficult task to implement. We have amended §§ 104.275 and 105.265 to clarify that cargo checks should be focused on the cargo, containers, or other cargo transport units arriving at or on the facility or vessel to detect evidence of tampering or to prevent cargo that is not meant for carriage from being accepted and stored at the facility without the knowing consent of the facility owner or

operator. Checking cargo containers may be limited to external examinations to detect signs of tampering, including checking of the integrity of seals; however screening the vehicle the cargo container arrives on remains a requirement under these regulations. The issue of cargo screening will be addressed by TSA, BCBP, and other appropriate agencies through programs such as the Customs-Trade Partnership Against Terrorism (C–TPAT), the Container Security Initiative (CSI), performance standards developed under section 111 of the MTSA, and the Secure Systems of Transportation (SST) under 46 U.S.C. 70116. The requirement to ensure the coordination of security measures with the shipper or other party aligns with the ISPS Code. It is intended that provisions be coordinated when there are regular or repeated cargo operations with the same shipper. This facilitates security between the shipper and the facility; therefore, we have made this type of coordination mandatory. We have, however, amended §§ 104.275(a)(5) and 105.265(a)(8) to clarify that this coordination is only required for frequent shippers. The requirements in § 105.265(a)(9) may be challenging to implement, but the requirements are consistent with the ISPS Code, part B. We believe that a continuous inventory of goods is important to the security of facilities, especially for those that handle dangerous goods or hazardous substances and may be involved in a transportation security incident.

Ten commenters were concerned about health and occupational safety during inspection of cargo spaces. Five commenters raised this concern in connection with tank barges, under the vessel security measures for handling cargo, § 104.275(b) and (c), and two other commenters raised the concern under the facility cargo-handling requirements in § 105.265(b)(1) and (b)(4).

Under § 104.275, we provide flexibility in how cargo spaces must be checked. This allows owners and operators to take safety into account in devising cargo check procedures. To emphasize safety during cargo operations, we have amended §§ 104.275(b)(1) and 105.265(b)(1) to reflect that a check on cargo and cargo spaces should be done unless it is unsafe to do so. We did not amend § 104.275(b)(4) in a similar manner because if the check of seals or other methods used to prevent tampering is unsafe for vessel personnel to conduct, they should liaise with the facility to ensure this is done.

Two commenters requested that § 104.275(a) describing the ''liaison'' between vessels and facilities during cargo transfers be amended to include the ''liaison'' between vessels and other vessels during ''vessel-to-vessel interfaces.''

We agree that a vessel-to-facility interface or a vessel-to-vessel activity could include cargo handling; therefore, we have amended § 104.275 to reflect vessel-to-vessel transfers of cargo in those paragraphs we believe require this clarification.

Three commenters asked the Coast Guard to issue guidance on using lighting to monitor a vessel underway. The commenters stated that lighting that diminishes the visibility of navigation lights will be detrimental to safety.

We believe that any lighting installed on board vessels must not compromise navigational safety. We do not intend at this time, however, to issue specific guidance on lighting. The Master is responsible for assuring that lighting installed for security monitoring does not interfere with navigational safety. Section 104.285(a)(2) lists the issues that must be considered when establishing the level and location of lighting. Section 104.285(a)(2)(iv) states that lighting effects, such as glare, and its impact on safety, navigation, and other security activities, must be considered.

One commenter stated that the monitoring requirements in § 104.285 conflict with crew rest periods necessary for the safe operation of the vessel.

We do not believe that § 104.285 conflicts with rest periods for crewmembers. It is the vessel owner's or operator's responsibility to ensure that manning levels are sufficient to implement the approved Vessel Security Plan at all MARSEC Levels. There are various ways to meet this requirement, including not operating the vessel at higher MARSEC Levels or limiting vessel operational hours, to ensure crew rest periods are maintained.

After further review of § 104.285(c)(5), we amended this paragraph to clarify that vessel owners or operators may need to include more than one of the additional security measures listed at MARSEC Level 2.

Three commenters suggested that we amend § 104.290(a)(1) to revise ''Prohibiting'' to read ''Deter to the best of their ability'' and § 104.290(a)(2) to revise ''Deny'' to read ''Denying access to the best of their ability.''

We disagree with the comments because the suggested changes would erode the level of security to be achieved by the regulations by providing an unenforceable standard.

Three commenters recommended that the notification procedures in § 104.290(a)(5) be amended to conform to 46 U.S.C. 70104 to include procedures for notifying and coordinating with local, State, and Federal authorities, including the Director of the Federal Emergency Management Agency.

We do not believe that it is necessary to amend § 104.290(a)(5) to align with 46 U.S.C. 70104. The statute is met through the AMS Plan, the implementation of which is intended to coordinate proper notification and response with shoreside authorities in the event of a transportation security incident. The COTP, as the Federal Maritime Security Coordinator, is responsible for notifications as discussed in subpart C of part 101.

One commenter asked how the Coast Guard defines ''critical vessel-to-facility interface operations'' that need to be maintained during transportation security incidents.

Section 104.290(a) requires vessel owners or operators to ensure that the Vessel Security Officer and vessel security personnel can respond to threats and breaches of security and maintain ''critical vessel and vessel-to-facility interface operations,'' while paragraph (e) of that section requires non-critical operations to be secured in order to focus response on critical operations. The Coast Guard does not define the critical operations that need to be maintained during security incidents, because these will vary depending on a vessel's physical and operational characteristics, but we do require each vessel to provide its own definition as part of its Vessel Security Plan. Section 104.305(d) requires that they discuss and evaluate in the Vessel Security Assessment report key vessel measures and operations, including operations involving other vessels or facilities.

One commenter suggested that commuter ticket books or badges could serve as a form of required identification for passengers on board ferries.

Personal identification remains a requirement in these regulations as described in § 101.515 to ensure, if needed, the identification of any passenger. A ticket book or badge that meets the requirements of § 101.515 could serve as personal identification. To ease congestion for ferry passengers, we have included alternatives to checking personal identification as described in § 104.292. These alternatives, if used, can expedite access

to the ferry while maintaining adequate security.

After further review, we amended § 104.292(d)(3) and § 104.292(e) to clarify which screening requirements the alternatives are replacing. We also added a requirement to § 104.292 for vessels using public access facilities, as that term is defined in part 101. These vessels must also address security measures for the interface with the public access facility. These amendments may be found in § 104.292(e)(3) and (f).

Two commenters requested that we amend § 104.297(c) to read ''port or place'' where a vessel owner or operator may have a vessel inspected, stating that many inspections do not take place in a port.

We believe that § 104.297(c) does not preclude a vessel from being inspected in a place other than a port. It is common industry practice for some inspections to take place in locations other than ports, and we do not believe the language in § 104.297(c) alters that practice.

Two commenters asked about the provisions in § 104.297 relating to the issuance of an ISSC to vessels on international voyages. One commenter recommended that an ISSC be issued to all ships as evidence of approval of a Vessel Security Plan, stating the issuance of a Vessel Security Plan letter of approval and an ISSC seems duplicative. One commenter also recommended that the inspection required in § 104.297(c) be combined with Certificate of Inspection examinations and that the ISSC be renewed as part of the Certificate of Inspection examinations.

We disagree that issuance of the Vessel Security Plan letter and an ISSC is duplicative. The Vessel Security Plan letter is issued by the Marine Safety Center upon review and approval of the Vessel Security Plan. The ISSC is issued by the COTP following verification that the Vessel Security Plan has been implemented on board the specific SOLAS vessel. We do not preclude combining the ISSC renewal examination with the Certificate of Inspection examination, as is currently done for verification and issuance of other international certificates. For non-SOLAS vessels, the verification that the Vessel Security Plan has been implemented on board the vessel will be done in conjunction with the Certificate of Inspection examination or any other regularly scheduled examination, if possible. If the non-SOLAS vessel is uninspected, the verification will occur during a separate examination.

One commenter questioned the need for ship alerting systems for foreign flag vessels and asked the Coast Guard to hold the requirement for ship alerting systems in ''abeyance'' until the question regarding ship-alerting systems could be answered by IMO.

As we noted in the preamble to the temporary interim rule (68 FR 39263) (part 101), the Coast Guard is considering applying ship alerting systems to U.S. domestic vessels not subject to SOLAS. Ship alerting systems for foreign flag vessels and U.S. flag vessels subject to SOLAS will be required by SOLAS amendment XI–2 (regulation 6). This comment, therefore, is beyond the scope of this regulation.

One commenter suggested that the temporary interim rule for Vessel Security incorrectly stated that the vessel must maintain and update the continuous synopsis record, contending that this is the flag administration's responsibility.

SOLAS Chapter XI–1, regulation 5, requires flag administrations to issue continuous synopsis records to vessels. Flag administrations must also update the continuous synopsis record based on information provided by the company or vessel. The flag administration must then issue these updated continuous synopsis records to the vessel. To enable flag administrations to perform this function, regulation 5 clearly requires the vessel owner or operator to provide the flag administration current information so that the continuous synopsis record can provide an accurate, on board record of the history of the vessel.

One commenter asked that the Coast Guard articulate how the continuous synopsis record is going to be provided to those vessels that may be subject to Port State Control outside the U.S. where other governments will be looking for one document, not a combination of the Certificate of Documentation and a Certificate of Inspection.

SOLAS Chapter XI–1, regulation 5, requires that the continuous synopsis record be in the format developed by the IMO. The IMO has not developed a format yet. We will comply with the IMO format once it has been adopted. We intend to issue a continuous synopsis record before July 2004. The currency of the information will be based primarily on the information provided by the owner or operator. Sanctions can be imposed for any inaccurate information provided by the owner or operator.

Two commenters encouraged the formal training of Coast Guard Port State Control officers in enforcing these regulations to include the details of security systems and procedures, security equipment, and the elements of knowledge required of the Vessel Security Officer and Facility Security Officer.

The Coast Guard conducts comprehensive training of its personnel involved in ensuring the safety and security of facilities and commercial vessels. We continually update our curriculum to encompass new requirements, such as the Port State Control provisions of the ISPS Code. This training, however, is beyond the scope of this rule.

*Subpart C–Vessel Security Assessment (VSA)*

This subpart describes the content and procedures for Vessel Security Assessments.

We received 22 comments pertaining to sensitive security information and its disclosure. Twelve commenters requested that the Coast Guard delete the requirements that the Facility Security Assessment or Vessel Security Assessment be included in the submission of the Facility Security Plan or Vessel Security Plan respectively, stating that the security assessments are of such a sensitive nature that risk of disclosure is too great. Four commenters stated that form CG–6025 ''Facility Vulnerability and Security Measures Summary'' should be sufficient for the needs of the Coast Guard and would promote facility security. Two commenters stated that there are too many ways for the general public to gain access to sensitive security information. One commenter stated that it was not clear how the Coast Guard would safeguard sensitive security information. One commenter stated that training for personnel in parts of the Facility Security Plan should not require access to the Facility Security Assessment.

Sections 104.405, 105.405, and 106.405 require that the security assessment report be submitted with the respective security plans. We believe that the security assessment report must be submitted as part of the security plan approval process because it is used to determine if the security plan adequately addresses the security requirements of the regulations. The information provided in form CG–6025 will be used to assist in the development of AMS Plans. The security assessments are not required to be submitted. To clarify that the report, not the assessment, is what must be submitted with the Vessel or Facility Security Plan, we are amending § 104.305 to add the word ''report''

where appropriate. We have also amended §§ 105.305 and 106.305 for facilities and OCS facilities, respectively. Additionally, we have amended these sections so that the Facility Security Assessment report requirements mirror the Vessel Security Assessment report requirements. All of these requirements were included in our original submission to OMB for ''Collection of Information'' approval, and there is no associated increase in burden in our collection of information summary. We also acknowledge that security assessments and security assessment reports have sensitive security information within them, and that they should be protected from unauthorized access under §§ 104.400(c), 105.400(c), and 106.400(c). Therefore, we are amending §§ 104.305, 105.305, and 106.305 to clarify that all security assessments, security assessment reports, and security plans need to be protected from unauthorized disclosure. The Coast Guard has already instituted measures to protect sensitive security information, such as security assessment reports and security plans, from disclosure.

Ten commenters addressed the disclosure of security plan information. One commenter seemed to advocate making security plans public. One commenter was concerned that plans will be disclosed under the Freedom of Information Act (FOIA). One commenter requested that mariners and other employees whose normal working conditions are altered by a Vessel or Facility Security Plan be granted access to sensitive security information contained in that plan on a need-to-know basis. One commenter stated that Company Security Officers and Facility Security Officers should have reasonable access to AMS Plan information on a need-to-know basis. One commenter stated that the Federal government must preempt State law in instances of sensitive security information because of past experience with State laws that require full disclosure of public documents. Three commenters supported our conclusion that the MTSA and our regulations preempt any conflicting State requirements. Another commenter is particularly pleased to observe the strong position taken by the Coast Guard in support of Federal preemption of possible State and local security regimes. One commenter supported our decision to designate security assessments and plans as sensitive security information.

Portions of security plans are sensitive security information and must be protected in accordance with 49 CFR part 1520. Only those persons specified in 49 CFR part 1520 will be given access to security plans. In accordance with 49 CFR part 1520 and pursuant to 5 U.S.C. 552(b)(3), sensitive security information is generally exempt from disclosure under FOIA, and TSA has concluded that State disclosure laws that conflict with 49 CFR part 1520 are preempted by that regulation. 46 U.S.C. 70103(d) also provides that the information developed under this regulation is not required to be disclosed to the public. However, §§ 104.220, 104.225, 105.210, 105.215, 106.215, and 106.220 of these rules state that vessel and facility personnel must have knowledge of relevant provisions of the security plan. Therefore, vessel and facility owners or operators will determine which provisions of the security plans are accessible to crewmembers and other personnel. Additionally, COTPs will determine what portions of the AMS Plan are accessible to Company or Facility Security Officers.

Information designated as sensitive security information is generally exempt under FOIA, and TSA has concluded that State disclosure laws that conflict with 49 CFR part 1520 are preempted by that regulation. 46 U.S.C. 70103(d) also provides that the information developed under this regulation is not required to be disclosed to the public.

Two commenters stated that our regulations suggest that information designated as sensitive security information is exempt from FOIA. One commenter suggested that all documentation submitted under this rule be done pursuant to the Homeland Security Act of 2002, to afford a more legally definite protection against disclosure.

''Sensitive security information'' is a designation mandated by regulations promulgated by TSA and may be found 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.

One commenter stated that the owners and operators of commercial vessels do not have the resources for additional work and paperwork requirements, believing that the rule will drive some owners and operators out of business.

The MTSA requires the owners or operators of vessels that may be involved in a transportation security incident to develop and implement security plans for their vessels. While these regulations will result in an increased burden for much of the maritime industry, we believe the rules are necessary to ensure maritime homeland security. We have developed these regulations to be as flexible as possible in their implementation, including allowing Alternative Security Programs and equivalencies, while still ensuring maritime security.

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 allows 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.

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, § 101.415.

We received three comments regarding the use of RSOs. Two commenters asked whether an RSO could complete a Vessel Security Assessment. One commenter stated that there is a good deal of confusion concerning the fact that an RSO may audit a Vessel Security Assessment and a Vessel Security Plan but cannot actually perform the assessment.

The Coast Guard is not designating any RSOs and will be approving and verifying implementation of all Vessel Security Plans. As provided in § 104.300(c), third parties may be used in any aspect of the Vessel Security Assessment if they have the appropriate skills and if the Company Security Officer reviews and accepts their work. The regulations do not prohibit any third party, including entities that have RSO status abroad, from performing an assessment or audit. However, the regulations prohibit a third party or any person responsible for implementing any security measures in the Vessel Security Plan from performing required audits. It should be noted that the ISPS Code prohibits an RSO that is involved in developing a Vessel Security Plan from reviewing or approving, on behalf of an Administration, the Vessel Security Plan.

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.

One commenter asked whether persons who have already completed the ''ISPS—Company Security Officers Course'' can be considered competent to carry out a shipboard assessment.

The owner or operator of a vessel may rely upon third parties to conduct the Vessel Security Assessment. Section 104.300(d) lists the areas in which anyone involved in a Vessel Security Assessment must have knowledge. While we have not examined the ''ISPS—Company Security Officers Course'' to determine whether it provides adequate training in the areas listed in § 104.300(d), an owner or operator may make that determination on their own in light of the regulatory and international competency requirements.

One commenter asked for clarification of the terms ''self assessments,'' ''security assessments,'' ''risk/threat assessments,'' and ''on-scene surveys.''

Risk/threat assessments and self assessments are not specifically defined in the regulations, but refer to the general practices of assessing where a vessel or facility is at risk. The assessments required in parts 104 through 106 must take into account threats, consequences, and vulnerabilities; therefore, they are most appropriately titled ''security assessments.'' This title also aligns with the ISPS Code. To clarify that §§ 101.510 and 105.205 address security assessments required by subchapter H, we have amended these sections to change the term ''risk'' to the more accurate term ''security.'' ''On-scene surveys'' are explained in the security assessment requirements of parts 104, 105, and 106. As explained in § 104.305(b), for example, the purpose of an on-scene survey is to ''verify or 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.

Three commenters asked how a company should assess the ''worse-case scenario'' regarding barges and their cargo.

There are various methods of conducting a security assessment, several of which we outlined in § 101.510. These assessment tools, the assessment requirements themselves as discussed in §§ 104.305, 105.305, and 106.305, and other assessment tools that have been developed by industry should enable owners or operators to evaluate the vulnerability and potential consequences of a transportation security incident involving the barge or the cargo it carries.

Two commenters asserted that the requirement in § 104.305(b) for an on-scene survey to be complete and plan submitted 60 days in advance of the vessel's operation is not reasonable because the vessel's crew and equipment may not yet be on board or installed.

We recognize the requirements of § 104.305(b) may pose challenges for owners and operators that intend to put their vessels into service after July 1, 2004. We believe the elements of a Vessel Security Assessment, as listed in § 104.305(a), can be addressed before the vessel comes into full operation. The purpose of part 104 is to ensure that an effective Vessel Security Plan is implemented before interfacing with facilities or other vessels. It would be imprudent to allow vessels to enter into service without Vessel Security Plans in place. Therefore, we have not amended this requirement and will only allow vessels to operate upon verification of the implementation of an approved Vessel Security Plan.

Three commenters requested that the Coast Guard amend preamble language to clarify which personnel may conduct a Vessel Security Assessment, stating that we were not clear in the temporary interim rule (68 FR 39240) (part 101).

As provided in § 104.210(a)(4), the Company Security Officer may delegate duties required in part 104, including conducting Vessel Security Assessments. The Company Security Officer remains responsible for the performance of all security-related duties, even when delegated. Under § 104.300(c), third parties may work on a Vessel Security Assessment so long as the Company Security Officer reviews and accepts their work.

One commenter noted that § 104.305(d)(2) requires that the Vessel Security Assessment report address, among other things, the structural integrity of the vessel, and that the implications of this requirement is that we will have non-naval architects commenting on the structural integrity of vessels built under existing rules and regulations. The commenter does not believe that there are counter-measures available for perceived shortcomings in the ship's construction standards and also asks if the Coast Guard anticipates using Vessel Security Assessments as a basis for proposals to amend SOLAS construction standards. Two commenters noted that, although required to assess their vulnerability of approaching recreational boats that may pose harm, vessels are not equipped to react to such a threat.

The provisions of § 104.305(d)(2) align with the ISPS Code, part B. The owner or operator is responsible for the Vessel Security Assessment and,

therefore, may have a naval architect or other qualified professional evaluate the structural integrity of the vessel in conducting the assessment. If, in evaluating the structural integrity of a vessel, the owner or operator determines that no security measures are available for perceived shortcomings in the ship's structural integrity, then the plan will not be required to contain any. We do not, at this time, anticipate using the Vessel Security Assessment as a basis for proposing amendments to SOLAS construction standards. With regard to approaching recreational boats, at higher MARSEC Levels, the owner or operator must implement appropriate security measures if the vessel is at risk from such a threat, such as changing operational schedule, using watercraft as a deterrence or coordinating with the facility for such use, or notifying the COTP or the NRC of a specific threat.

After further review of subpart C of parts 104, 105, and 106, we amended §§ 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 re-approval.

*Subpart D—Vessel Security Plan (VSP)*

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

Two commenters asked the Coast Guard to change the language in § 104.400(a) to delineate the responsibilities of towing vessels and facilities when dealing with unmanned vessels.

We are amending the definition of ''owner or operator'' in § 101.105 to clarify when ''operational control'' of unmanned vessels passes between vessels and facilities. No change was made to § 104.400(a) because the change to the definition of ''owner or operator'' addresses this concern.

One commenter suggested the Coast Guard change the definition of Vessel Security Plan to read verbatim from the MTSA.

Our definition of Vessel Security Plan is consistent with the MTSA, and we believe that it provides clarity on the purpose of the plan.

One commenter stated that Vessel Security Plans should contain a statement recognizing the authority of the Coast Guard to require security measures to deter a transportation security incident and acknowledging that the owner or operator will ensure, by contract or other approved means, the availability of the particular security measures when and if specifically designated and required by the Coast Guard.

The MTSA provided the authority for us to require additional security; however, the Vessel Security Plan need not contain a statement recognizing the authority of the Coast Guard. Under § 104.240(b)(1), we state that the vessel owner or operator must ensure that whenever a higher MARSEC Level is set for the port in which the vessel is located or is about to enter, the vessel complies, without undue delay, with all measures specified in the Vessel Security Plan. Section 104.240(e) requires that, at MARSEC Level 3, the owner or operator must be able to implement additional security measures. The Vessel Security Plan need only describe how the owner or operator will meet the requirements in § 104.240; the statement ''by contract or other approved means'' is not required.

One commenter stated that as part of developing a Vessel Security Plan, the commenter would have to contract, in advance, with shore-based companies for security measures and anti-terrorism services.

Nothing in these regulations requires that vessel owners or operators contract for such services in advance. However, if an owner or operator of a vessel develops and has approved a Vessel Security Plan that states it will hire shore-based companies to provide certain security measures, then the vessel owner or operator must be prepared to demonstrate that the plan can be implemented as approved. It is the intent of these regulations that vessel owners or operators, in accordance with their Vessel Security Assessments, identify those resources they will need at the various MARSEC Levels to ensure that they can implement their Vessel Security Plans.

One commenter recommended that a ''working language'' provision be added to the regulation to ensure that the Vessel Security Plan is understood by the crew that is responsible for its implementation. One commenter recommended that the Coast Guard amend the requirements of part 104 to include a provision to encourage foreign vessels to carry a copy of their Vessel Security Plan written in English. This commenter believed that Coast Guard Port State Control officers may be delayed when they encounter a Vessel Security Plan written in a language other than English.

We agree that a plan written in a language other than English may cause a delay during a Port State Control examination. However, we believe that all vessel personnel must have knowledge of security-related measures as specified in the Vessel Security Plan. We agree, therefore, that providing the Vessel Security Plan or sections of the Vessel Security Plan in the working language of the crew is good maritime practice. While we require that the Vessel Security Plan be submitted in English, we are amending § 104.400 to also encourage the owner or operator of a vessel to provide a translation in the working language of the crew to ensure that vessel personnel can perform their security duties. We are also amending § 104.410 to clarify that we require Vessel Security Plans to be submitted to the MSC in English. Additionally, to meet our international obligations we do not require that foreign vessels carry on board the vessel a copy of its Vessel Security Plan written in English. Part A of the ISPS Code permits Vessel Security Plans to be written in the working language or languages of the ship, so long as a translation of the plan is provided in English, Spanish, or French. As we stated in the preamble of the temporary interim rule (68 FR 39297) (part 101), a vessel may be delayed while translator services are acquired when a Port State Control officer is presented a Vessel Security Plan in a language that he or she does not understand. Although not required, it would help our Port State Control efforts if the plan were maintained in English as well.

One commenter recommended that the provisions for the MTSA, requiring Vessel Security Plans to be consistent with the National and AMS Plans, be waived until both of these plans exist.

We cannot waive a legislative requirement without express authority to do so. However, we do not anticipate that Vessel Security Plans or Facility Security Plans will need to be resubmitted or revised when the National and AMS Plans are developed. We view the regulatory requirements for Vessel Security Plans and Facility Security Plans to be the fundamental building blocks for these broader plans.

One commenter stated that an outline for Vessel Security Plans should be provided similar to the one in § 105.405 for Facility Security Plans.

We believe that the format for the Vessel Security Plans provided in § 104.405 is complete and differs little from the one provided in § 105.405.

Three commenters recommended that the regulations 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 before and after July 1, 2004.

One commenter suggested that the Coast Guard amend § 104.410(a) to read: ''each vessel owner or operator, where required, must either'' instead of ''each vessel owner or operator must either.''

We disagree with the comment because we feel that the current language best conveys the intent of the regulation. We believe that it is clear that this part is applicable only to those owners or operators who are required to submit a security plan.

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.

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), 105.410(a)(2), 106.410(a)(2), 105.115(a), and 106.110(a) to clarify the submission requirements for the Alternative Security Program.

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 regulations state that the security plan must be audited if there have been significant modifications to the vessel or facility, including, but not limited to, their physical structure, emergency response procedures, security measures, or operations. These all represent significant modifications. Therefore, we are not going to create an exception in the regulation. We recognize that the regulations requiring that proposed amendments to security plans be submitted for approval 30 days before implementation could be construed as an impediment to taking necessary security measures in a timely manner. The intent of this requirement is to ensure that amendments to the security plans are reviewed to ensure they are consistent with and supportable by the security assessments. It is not intended to be, nor should it be, interpreted as precluding the owner or operator from the timely implementation of additional security measures above and beyond those enumerated in the approved security plan to address exigent security situations. Accordingly we have amended §§ 104.415, 105.415, and 106.415 to add a clause that allows for the immediate implementation of additional security measures to address exigent security situations.

One commenter stated that vessel owners and operators should be allowed to amend Vessel Security Plans through annual letters to the Coast Guard, stating that Vessel Security Plans should be living documents that can be readily changed to reflect audit findings and lessons learned from drills and exercises. One commenter requested a definition for the scope of a plan change that constitutes an amendment to a Vessel Security Plan.

We agree that the Vessel Security Plan is a living document that should be continuously updated to incorporate changes or lessons learned from drills and exercises, and the regulations currently allow for frequent audit and amendments. We believe, however, that any changes to Vessel Security Plans should be submitted to the Coast Guard as soon as practicable, which may require more than an annual letter. In addition, we require that vessel owners and operators submit changes to the Marine Safety Center for review 30 days before the change becomes effective to ensure changes are consistent with the regulations.

Five commenters asked about the need for independent auditors under §§ 104.415 and 105.415. Two commenters recommended that we amend § 105.415(b)(4)(ii) to read ''not have regularly assigned duties for that facility'' as this would allow flexibility for audits to be conducted by individuals with security-related duties as long as those duties are not at that facility.

We believe that independent auditors are one, but not the only, way to conduct audits of Facility Security Plans. In both §§ 104.415 and 105.415, paragraph (b)(4) lists three requirements for auditors that, for example, could be met by employees of the same owner or operator who do not work at the facility or on the vessel where the audit is being conducted. Additionally, paragraph (b)(4) states that all of these requirements do not need to be met if impracticable due to the facility's size or the nature of the company.

*Miscellaneous*

Two commenters recommended that the regulations be amended to clarify the authority of the cognizant Officer in Charge of Marine Inspection to issue the ISSC to qualifying vessels.

To clarify this authority, we have added 46 CFR 2.01–25(a)(2)(viii).

After further review of this part we made several non-substantive editorial changes, such as adding plurals and fixing noun, verb, and subject agreements. These sections include: §§ 104.200(b)(14)(i), 104.215(a)(3), 104.265(b)(1) and (c)(5), 104.270(b)(5), 104.285(a)(1)(i), and 104.305(d)(3)(iv). In addition, the part heading in this part has been amended to align with all the part headings within this subchapter.

**Regulatory Assessment**

This final rule is a ''significant regulatory action'' under section 3(f) of

Executive Order 12866, Regulatory Planning and Review. The Office of Management and Budget has reviewed it under that Order. It requires an assessment of potential costs and benefits under section 6(a)(3) of that Order. It is significant under the regulatory policies and procedures of the Department of Homeland Security. A final assessment is available in the docket as indicated under **ADDRESSES**. A summary of comments on the assessment, our responses, and a summary of the assessment follow.

Five commenters stated that our cost estimates understate the cost for international ships calling on U.S. ports. Three commenters noted that the same parameters used to develop the costs for the U.S. SOLAS ships should be extrapolated and applied to international ships, adjusted for the time these ships spend in U.S. waters. One commenter asked us to explain why only 70 foreign flag vessels were included in our analysis of the cost of the temporary interim rule.

We disagree with the commenters' assertion that our estimate understates the cost for international ships calling on U.S. ports. We developed our estimate assuming that foreign flag vessels subject to SOLAS would be required by their flag state, as signatories to SOLAS, to implement SOLAS and the ISPS Code. The flag administrations of foreign flag SOLAS vessels will account, therefore, for the costs of complying with SOLAS and the ISPS Code. Our analysis accounts for the costs of this rule to U.S. flag vessels subject to SOLAS. Additionally, we estimate costs for the approximately 70 foreign flag vessels that are not subject to SOLAS that would not need to comply with either SOLAS or the ISPS Code. These vessels must comply with the requirements in 33 CFR part 104 if they wish to continue operating in U.S. ports after July 1, 2004, and we therefore estimate the costs to these vessels.

One commenter suggested that cost assessments for auditing the Vessel Security Assessment and Vessel Security Plan be revisited, stating that the present 15-minute cost estimate to update the Vessel Security Plan did not account for the expense of an annual review and audit.

The estimated average incremental cost for the 15-minute update of the Vessel Security Plan accounts for the time a Company Security Officer or Vessel Security Officer spends making minor changes. The cost of an annual review and audit cost is incurred at the company, not the vessel, level. We have accounted for this cost for both large and small companies. We also assumed that, for large companies operating vessels subject to SOLAS, the cost would be incremental to existing expenses for annual audits already required under the International Safety Management Code and other international instruments. For further detail on the cost calculations, see the Cost Assessment and Final Regulatory Flexibility Act analysis in the docket for this rule.

One commenter suggested taking into greater account the risk factors of the facility and vessel as a whole, rather than simply relying on one factor, such as the capacity of a vessel as well as the cost-benefit of facility security to all of the business entities that make up a facility.

The Coast Guard considered an extensive list of risk factors when developing these regulations including, but not limited to, vessel and facility type, the nature of the commerce in which the entity is engaged, potential trade routes, accessibility of facilities, gross tonnage, and passenger capacity. Our Cost Assessments and Regulatory Flexibility Act Analyses for both the temporary interim rules and the final rules are available in the docket, and they account for companies as whole business entities, not individual vessels or facilities.

*Cost Assessment*

For the purposes of good business practice or pursuant to regulations promulgated by other Federal and State agencies, many companies already have spent a substantial amount of money and resources to upgrade and improve security. The costs shown in this assessment do not include the security measures these companies have already taken to enhance security. Because the changes in this final rule do not affect the original cost estimates presented in the temporary interim rule (68 FR 39298) (part 104), the costs remain unchanged.

We realize that every company engaged in maritime commerce would not implement the final rule exactly as presented in this assessment. Depending on each company's choices, some companies could spend much less than what is estimated herein while others could spend significantly more. In general, we assume that each company would implement the final rule based on the type of vessels or facilities it owns or operates and whether it engages in international or domestic trade.

This assessment presents the estimated cost if vessels are operating at MARSEC Level 1, the current level of operations since the events of September 11, 2001. We also estimated the costs for operating for a brief period at MARSEC Level 2, an elevated level of security.

We do not anticipate that implementing the final rule will require additional manning on board vessels; existing personnel can assume the duties envisioned.

The final rule will affect about 10,300 U.S. flag SOLAS and domestic (non-SOLAS) vessels, and about 70 foreign non-SOLAS vessels.

The estimated cost of complying with the final rule is present value $1.368 billion (2003–2012, 7 percent discount rate). Approximately present value $248 million of this total is attributable to U.S. flag SOLAS vessels. Approximately present value $1.110 billion is attributable to domestic vessels (non-SOLAS), and present value $10 million is attributable to foreign non-SOLAS vessels. In the first year of compliance, the cost of purchasing equipment, hiring security officers, and preparing paperwork is an estimated $218 million (non-discounted, $42 million for the U.S. flag SOLAS fleet, $175 million for the domestic fleet, $1 million for the foreign non-SOLAS fleet). Following initial implementation, the annual cost of compliance is an estimated $176 million (non-discounted, $32 million for the U.S. flag SOLAS fleet, $143 million for the domestic fleet, $1 million for the foreign non-SOLAS fleet).

For the U.S. flag SOLAS fleet, approximately 52 percent of the initial cost is for hiring Company Security Officers and training personnel, 29 percent is for vessel equipment, 12 percent is for assigning Vessel Security Officers to vessels, and 7 percent is associated with paperwork (Vessel Security Assessment and Vessel Security Plan). Following the first year, approximately 72 percent of the cost is for Company Security Officers and personnel training, 3 percent is for vessel equipment, 10 percent is for drilling, 15 percent is for Vessel Security Officers, and less than 1 percent is associated with paperwork. Company Security Officers and training are the primary cost drivers for U.S. flag SOLAS vessels.

For the domestic fleet, approximately 51 percent of the initial cost is for hiring Company Security Officers and training personnel, 29 percent is for vessel equipment, 14 percent is for assigning Vessel Security Officers to vessels, and 6 percent is associated with paperwork (Vessel Security Assessments and Vessel Security Plans). Following the first year, approximately 61 percent of the cost is for Company Security Officers and training, 6 percent is for vessel equipment, 11 percent is for

drilling, 22 percent is for VSOs, and less than 1 percent is associated with paperwork. As with SOLAS vessels, Company Security Officers are the primary cost driver for the domestic fleet.

We estimated approximately 135,000 burden hours for paperwork during the first year of compliance (33,000 hours for U.S. flag SOLAS, 101,000 hours for the domestic fleet, 1,000 hours for the foreign non-SOLAS fleet). We estimated approximately 12,000 burden hours annually following full implementation of the final rule (2,000 hours for U.S. flag SOLAS, 10,000 hours for the domestic fleet, less than 1,000 hours for the foreign non-SOLAS fleet).

We also estimated the annual cost for going to an elevated security level, MARSEC Level 2, in response to increased threats. The duration of the increased threat level will be entirely dependent on intelligence received. For this assessment, we estimated costs for MARSEC Level 2 using the following assumptions: All ports will go to MARSEC Level 2 at once, each elevation will last 21 days, and the elevation will occur twice a year. The estimated cost associated with these conditions is $235 million annually.

*Benefit Assessment*

This final rule is one of six final rules that implement national maritime security initiatives concerning general provisions, Area Maritime Security, vessels, facilities, Outer Continental Shelf (OCS) facilities, and AIS. The Coast Guard used the National Risk Assessment Tool (N–RAT) to assess benefits that would result from increased security for vessels, facilities, OCS facilities, and areas. The N–RAT considers threat, vulnerability, and consequences for several maritime entities in various security-related scenarios. For a more detailed discussion on the N–RAT and how we employed this tool, refer to ''Applicability of National Maritime Security Initiatives'' in the temporary interim rule titled ''Implementation of National Maritime Security Initiatives'' (68 FR 39243) (part 101). For this benefit assessment, the Coast Guard used a team to calculate a risk score for each entity and scenario before and after the implementation of required security measures. The difference in before and after scores indicated the benefit of the proposed action.

We recognized that the final rules are a ''family'' of rules that will reinforce and support one another in their implementation. We have ensured, however, that risk reduction that is credited in one rule is not also credited in another. For a more detailed discussion on the benefit assessment and how we addressed the potential to double-count the risk reduced, refer to ''Benefit Assessment'' in the temporary interim rule titled ''Implementation of National Maritime Security Initiatives'' (68 FR 39274) (part 101).

We determined annual risk points reduced for each of the six final rules using the N–RAT. The benefits are apportioned among the Vessel, Facility, OCS Facility, AMS, and AIS requirements. As shown in Table 1, the implementation of vessel security for the affected population reduces 781,285 risk points annually through 2012. The benefits attributable for part 101, General Provisions, were not considered separately since it is an overarching section for all the parts.

TABLE 1.—ANNUAL RISK POINTS REDUCED BY THE FINAL RULES

| Maritime entity | Annual risk points reduced by final fule | | | | |
|---|---|---|---|---|---|
| | Vessel security | Facility security | OCS Facility security | AMS | AIS |
| Vessels | 778,633 | 3,385 | 3,385 | 3,385 | 1,317 |
| Facilities | 2,025 | 469,686 | ..... | 2,025 | ..... |
| OCS Facilities | 41 | ..... | 9,903 | ..... | ..... |
| Port Areas | 587 | 587 | ..... | 129,792 | 105 |
| Total | 781,285 | 473,659 | 13,288 | 135,202 | 1,422 |

Once we determined the annual risk points reduced, we discounted these estimates to their present value (7 percent discount rate, 2003–2012) so that they could be compared to the costs. We presented the cost effectiveness, or dollars per risk point reduced, in two ways: First, we compared the first-year cost and first-year benefit because first-year cost is the highest in our assessment as companies develop security plans and purchase equipment. Second, we compared the 10-year present value cost and the 10-year present value benefit. The results of our assessment are presented in Table 2.

TABLE 2.—FIRST-YEAR AND 10-YEAR PRESENT VALUE COST AND BENEFIT OF THE FINAL RULES

| Item | Final rule | | | | |
|---|---|---|---|---|---|
| | Vessel security | Facility security | OCS facility security | AMS | AIS* |
| First-Year Cost (millions) | $218 | $1,125 | $3 | $120 | $30 |
| First-Year Benefit | 781,285 | 473,659 | 13,288 | 135,202 | 1,422 |
| First-Year Cost Effectiveness ($/Risk Point Reduced) | 279 | 2,375 | 205 | 890 | 21,224 |
| 10-Year Present Value Cost (millions) | 1,368 | 5,399 | 37 | 477 | 26 |
| 10-Year Present Value Benefit | 5,871,540 | 3,559,655 | 99,863 | 1,016,074 | 10,687 |
| 10-Year Present Value Cost Effectiveness ($/Risk Point Reduced) | 233 | 1,517 | 368 | 469 | 2,427 |

*Cost less monetized safety benefit.

**Small Entities**

Under the Regulatory Flexibility Act (5 U.S.C. 601–612), we have considered whether this final rule would have a significant economic impact on a substantial number of small entities. The term ''small entities'' comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000.

We found that the facilities (part 105), vessels (part 104), and AIS rules may have a significant impact on a substantial number of small entities. However, we were able to certify no significant economic impact on a substantial number of small entities for the Area Maritime Security (part 103) and OCS facility security (part 106) rules. A complete small entity analysis may be found in the ''Cost Assessment and Final Regulatory Flexibility Analysis'' for these rules.

We received comments regarding small entities; these comments are discussed within the ''Discussion of Comments and Changes'' section of this final rule.

*U.S. Flag SOLAS Vessels.*

We estimated that 88 companies that own U.S. flag SOLAS vessels will be affected by the final rule. We researched these companies and found revenue data for 32 of them (36 percent). The revenue impacts for these vessels are presented in Table 3. In this analysis, we considered the impacts to small businesses during the first year of implementation, when companies will be conducting assessments, developing security plans, and purchasing equipment. We also considered annual revenue impacts following the first year, when companies will have the assessments and plans complete, but will need to conduct quarterly drilling.

TABLE 3.—ESTIMATED REVENUE IMPACTS FOR SMALL BUSINESSES THAT OWN U.S. FLAG SOLAS VESSELS

| Percent impact on annual revenue | Initial | | Annual | |
|---|---|---|---|---|
| | Number of small entities with known revenue data | Percent of small entities with known revenue data | Number of small entities with known revenue data | Percent of small entities with known revenue data |
| 0–3 | 8 | 25 | 8 | 25 |
| 3–5 | 3 | 9 | 3 | 9 |
| 5–10 | 1 | 3 | 4 | 13 |
| 10–20 | 6 | 19 | 4 | 13 |
| 20–30 | 4 | 13 | 3 | 9 |
| 30–40 | 1 | 3 | 2 | 6 |
| 40–50 | 3 | 9 | 2 | 6 |
| > 50 | 6 | 19 | 6 | 19 |
| Total | 32 | 100 | 32 | 100 |

We assume that the remaining 56 entities that did not have revenue data are very small businesses. We assume that the final rule may have a significant economic impact on these businesses.

*Domestic Vessels*

We estimated that 1,683 companies that own domestic vessels will be affected by the final rule. We researched these companies and found revenue data for 822 of them (49 percent). The revenue impacts for these vessels are presented in Table 4. As with U.S. flag SOLAS vessels, we considered the impacts to small businesses during the first year of implementation, when companies will be conducting assessments, developing security plans, and purchasing equipment. We also considered annual revenue impacts following the first year, when companies will have the assessments and plans complete, but will need to conduct quarterly drilling.

TABLE 4.—ESTIMATED REVENUE IMPACTS FOR SMALL BUSINESSES THAT OWN DOMESTIC VESSELS

| Percent impact on annual revenue | Initial | | Annual | |
|---|---|---|---|---|
| | Number of small entities with known revenue data | Percent of small entities with known revenue data | Number of small entities with known revenue data | Percent of small entities with known revenue data |
| 0–3 | 366 | 45 | 393 | 48 |
| 3–5 | 86 | 10 | 87 | 11 |
| 5–10 | 171 | 21 | 170 | 21 |
| 10–20 | 85 | 10 | 64 | 8 |
| 20–30 | 34 | 4 | 37 | 5 |
| 30–40 | 19 | 2 | 16 | 2 |
| 40–50 | 9 | 1 | 16 | 2 |
| > 50 | 52 | 6 | 39 | 5 |
| Total | 822 | 100 | 822 | 100 |

We assumed that the remaining 861 entities that did not have revenue data are very small businesses. We assumed that the final rule may have a significant economic impact on these businesses.

*Assistance for Small Entities*

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Public Law 104–121), we offered to assist small entities in understanding the rule so that they could better evaluate its effects on them and participate in the rulemaking. We provided small entities with a name, phone number, and e-mail address to contact if they had questions concerning the provisions of the final rules or options for compliance.

We have placed Small Business Compliance Guides in the dockets for the Area Maritime, Vessel, and Facility Security and the AIS rules. These Compliance Guides will explain the applicability of the regulations, as well as the actions small businesses will be required to take in order to comply with each respective final rule. We have not created Compliance Guides for part 101 or for the OCS Facility Security final rule, as neither will affect a substantial number of small entities.

Small businesses may send comments on the actions of Federal employees who enforce, or otherwise determine compliance with, Federal regulations to the Small Business and Agriculture Regulatory Enforcement Ombudsman and the Regional Small Business Regulatory Fairness Boards. The Ombudsman evaluates these actions annually and rates each agency's responsiveness to small business. If you wish to comment on actions by employees of the Coast Guard, call 1–888–REG–FAIR (1–888–734–3247).

**Collection of Information**

This final rule contains no new collection of information requirements under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520). As defined in 5 CFR 1320.3(c), ''collection of information'' comprises reporting, recordkeeping, monitoring, posting, labeling, and other similar actions. The final rules are covered by two existing OMB-approved collections—1625–0100 [formerly 2115–0557] and 1625–0077 [formerly 2115–0622].

We received comments regarding collection of information; these comments are discussed within the ''Discussion of Comments and Changes'' section of this preamble. You are not required to respond to a collection of information unless it displays a currently valid OMB control number. We received OMB approval for these collections of information on June 16, 2003. They are valid until December 31, 2003.

**Federalism**

Executive Order 13132 requires the Coast Guard to develop an accountable process to ensure ''meaningful and timely input by State and local officials in the development of regulatory policies that have federalism implications.'' ''Policies that have federalism implications'' is defined in the Executive Order to include regulations that have ''substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.'' Under the Executive Order, the Coast Guard may construe a Federal statute to preempt State law only where, among other things, the exercise of State authority conflicts with the exercise of Federal authority under the Federal statute.

This action has been analyzed in accordance with the principles and criteria in the Executive Order, and it has been determined that this final rule does have Federalism implications and a substantial direct effect on the States. This final rule requires those States that own or operate vessels or facilities that may be involved in a transportation security incident to conduct security assessments of their vessels and facilities and to develop security plans for their protection. These plans must contain measures that will be implemented at each of the three MARSEC Levels and must be reviewed and approved by the Coast Guard.

Additionally, the Coast Guard has reviewed the MTSA with a view to whether we may construe it as non-preemptive of State authority over the same subject matter. We have determined that it would be inconsistent with the federalism principles stated in the Executive Order to construe the MTSA as not preempting State regulations that conflict with the regulations in this final rule. This is because owners or operators of facilities and vessels—that are subject to the requirements for conducting security assessments, planning to secure their facilities and vessels against threats revealed by those assessments, and complying with the standards, both performance and specific construction, design, equipment, and operating requirements—must have one uniform, national standard that they must meet. Vessels and shipping companies, particularly, would be confronted with an unreasonable burden if they had to comply with varying requirements as they moved from State to State. Therefore, we believe that the federalism principles enumerated by the Supreme Court in *U.S.* v. *Locke*, 529 U.S. 89 (2000) regarding field preemption of certain State vessel safety, equipment, and operating requirements extends equally to this final rule, especially regarding the longstanding history of significant Coast Guard maritime security regulation and control of vessels for security purposes. But, the same considerations apply to facilities, at least insofar as a State law or regulation applicable to the same subject for the purpose of protecting the security of the facility would conflict with a Federal regulation; in other words, it would either actually conflict or would frustrate an overriding Federal need for uniformity.

Finally, it is important to note that the regulations implemented by this final rule bear on national and international commerce where there is no constitutional presumption of concurrent State regulation. Many aspects of these regulations are based on the U.S. international treaty obligations regarding vessel and port facility security contained in SOLAS and the complementary ISPS Code. These international obligations reinforce the need for uniformity regarding maritime commerce.

Notwithstanding the foregoing preemption determinations and findings, the Coast Guard has consulted extensively with appropriate State officials, as well as private stakeholders during the development of this final rule. For these final rules, we met with the National Conference of State Legislatures (NCSL) Taskforce on Protecting Democracy on July 21, 2003, and presented briefings on the temporary interim rules to the NCSL's Transportation Committee on July 23, 2003. We also briefed several hundred State legislators at the American Legislative Exchange Council on August 1, 2003. We held a public meeting on July 23, 2003, with invitation letters to all State homeland security representatives. A few State representatives attended this meeting and submitted comments to a public docket prior to the close of the comment period. The State comments to the docket focused on a wide range of concerns including consistency with international requirements and the protection of sensitive security information.

One commenter stated that there should be national uniformity in implementing security regulations on international shipping.

As stated in the temporary interim rule for part 101 (68 FR 39277), we believe that the federalism principles

enumerated by the Supreme Court in *U.S.* v. *Locke,* 529 U.S. 89 (2000), regarding field preemption of certain State vessel safety, equipment, and operating requirements extends equally to this final rule, especially regarding the longstanding history of significant Coast Guard maritime security regulations and control of vessels for security purposes. It would be inconsistent with the federalism principles stated in Executive Order 13132 to construe the MTSA as not preempting State regulations that conflict with these regulations. Vessels and shipping companies, particularly, would be confronted with an unreasonable burden if they had to comply with varying requirements as they move from state to state.

One commenter stated that there is a ''real cost'' to implementing security measures, and it is significant. The commenter stated that there is a disparity between Federal funding dedicated to air transportation and maritime transportation and that the Federal government should fund maritime security at a level commensurate with the relative security risk assigned to the maritime transportation mode. Further, the commenter stated that, in 2002, some State-owned ferries carried as many passengers as one of the State's busiest international airports and provided unique mass transit services; therefore, the commenter supported the Alternative Security Program provisions of the temporary interim rule to enable a tailored approach to security.

The viability of a ferry system to provide mass transit to a large population is undeniable and easily rivals other transportation modes. We developed the Alternative Security Program to encompass operations such as ferry systems. We recognize the concern about the Federal funding disparity between the maritime transportation mode and other modes; however, this disparity is beyond the scope of this rule.

One commenter stated that while he appreciated the urgency of developing and implementing maritime security plans, the State would find it difficult to complete them based on budget cycles and building permit requirements. At the briefings discussed above, several NCSL representatives also voiced concerns over the short implementation period. In contrast, other NCSL representatives were concerned that security requirements were not being implemented soon enough.

The implementation timeline of these final rules follows the mandates of the MTSA and aligns with international implementation requirements. While budget-cycle and permit considerations are beyond the scope of this rule, the flexibility of these performance-based regulations should enable the majority of owners and operators to implement the requirements using operational controls, rather than more costly physical improvement alternatives.

Other concerns raised by the NCSL at the briefings mentioned above included questions on how the Coast Guard will enforce security standards on foreign flag vessels and how multinational crewmember credentials will be checked.

We are using the same cooperative arrangement that we have used with success in the safety realm by accepting SOLAS certificates documenting flag-state approval of foreign SOLAS Vessel Security Plans that comply with the comprehensive requirements of the ISPS Code. The consistency of the international and domestic security regimes, to the extent possible, was always a central part of the negotiations for the MTSA and the ISPS Code. In the MTSA, Congress explicitly found that ''it is in the best interests of the U.S. to implement new international instruments that establish'' a maritime security system. We agree and will exercise Port State Control to ensure that foreign vessels have approved plans and have implemented adequate security standards on which these rules are based. If vessels do not meet our security requirements, the Coast Guard may prevent those vessels from entering the U.S. or take other necessary measures that may result in vessel delays or detentions. The Coast Guard will not hesitate to exercise this authority in appropriate cases. We discuss the ongoing initiatives of ILO and the requirements under the MTSA to develop seafarers' identification criteria in the temporary interim rule titled ''Implementation of National Maritime Security Initiatives'' (68 FR 39264) (part 101). We will continue to work with other agencies to coordinate seafarer access and credentialing issues. These final rules will also ensure that vessel and facility owners and operators take an active role in deterring unauthorized access.

One commenter, as well as participants of the NCSL, noted that some State constitutions afford greater privacy protections than the U.S. Constitution and that, because State officers may conduct vehicle screenings, State constitutions will govern the legality of the screening. The commenter also noted that the regulations provide little guidance on the scope of vehicle screening required under the regulations.

The MTSA and this final rule are consistent with the liberties provided by the U.S. Constitution. If a State constitutional provision frustrates the implementation of any requirement in the final rule, then the provision is preempted pursuant to Article 6, Section 2, of the U.S. Constitution. The Coast Guard intends to coordinate with TSA and BCBP in publishing guidance on screening.

**Unfunded Mandates Reform Act**

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular, the Act addresses actions that may result in the expenditure by a State, local, or Indian Tribal government, in the aggregate, or by the private sector of $100,000,000 or more in any one year. This final rule is exempted from assessing the effects of the regulatory action as required by the Act because it is necessary for the national security of the United States (2 U.S.C. 1503(5)).

We did not receive comments regarding the Unfunded Mandates Reform Act.

**Taking of Private Property**

This final rule will not effect a taking of private property or otherwise have taking implications under Executive Order 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights. We did not receive comments regarding the taking of private property.

**Civil Justice Reform**

This final rule meets applicable standards in sections 3(a) and 3(b)(2) of Executive Order 12988, Civil Justice Reform, to minimize litigation, eliminate ambiguity, and reduce burden. We did not receive comments regarding Civil Justice Reform.

**Protection of Children**

We have analyzed this final rule under Executive Order 13045, Protection of Children from Environmental Health Risks and Safety Risks. While this final rule is an economically significant rule, it does not create an environmental risk to health or risk to safety that may disproportionately affect children. We did not receive comments regarding the protection of children.

**Indian Tribal Governments**

This final rule does not have tribal implications under Executive Order

13175, Consultation and Coordination with Indian Tribal Governments, because it does not have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes. We did not receive comments regarding Indian Tribal Governments.

**Energy Effects**

We have analyzed this final rule under Executive Order 13211, Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use. We have determined that it is not a ''significant energy action'' under that order. Although it is a ''significant regulatory action'' under Executive Order 12866, it is not likely to have a significant adverse effect on the supply, distribution, or use of energy. The Administrator of the Office of Information and Regulatory Affairs has not designated it as a significant energy action. Therefore, it does not require a Statement of Energy Effects under Executive Order 13211.

This final rule has a positive effect on the supply, distribution, and use of energy. The final rule provides for security assessments, plans, procedures, and standards, which will prove beneficial for the supply, distribution, and use of energy at increased levels of maritime security.

We did not receive comments regarding energy effects.

**Environment**

We have considered the environmental impact of this final rule and concluded that under figure 2–1, paragraphs (34)(a), (34)(c), and (34)(d), of Commandant Instruction M16475.lD, this final rule is categorically excluded from further environmental documentation. This final rule concerns security assessments, plans, training, and the establishment of security positions that will contribute to a higher level of marine safety and security for vessels and U.S. ports. A ''Categorical Exclusion Determination'' is available in the docket where indicated under **ADDRESSES** or **SUPPLEMENTARY INFORMATION**.

This final rule will not significantly impact the coastal zone. Further, the execution of this final rule will be done in conjunction with appropriate state coastal authorities. The Coast Guard will, therefore, comply with the requirements of the Coastal Zone Management Act while furthering its intent to protect the coastal zone.

We did not receive comments regarding the environment.

**List of Subjects**

*33 CFR Part 104*

Incorporation by reference, Maritime security, Reporting and recordkeeping requirements, Security measures, Vessels.

*33 CFR Part 160*

Administrative practice and procedure, Harbors, Hazardous material transportation, Marine safety, Navigation (water), Reporting and recordkeeping requirement, Vessels, Waterways.

*33 CFR Part 165*

Harbors, Marine safety, Navigation (water), Reporting and recordkeeping requirements, Security measures, Waterways.

*46 CFR Part 2*

Marine safety, Maritime security, Reporting and recordkeeping requirements, Vessels.

*46 CFR Part 31*

Cargo vessels, Inspection and certification, Maritime security.

*46 CFR Part 71*

Inspection and certification, Maritime security, Passenger vessels.

*46 CFR Part 91*

Cargo vessels, Inspection and Certification, Maritime security.

*46 CFR Part 115*

Fire prevention, Inspection and certification, Marine safety, Maritime security, Reporting and recordkeeping requirements, Vessels.

*46 CFR Part 126*

Cargo vessels, Inspection and certification, Marine safety, Maritime security, Reporting and recordkeeping requirements.

*46 CFR Part 176*

Fire prevention, Inspection, Marine safety, Maritime security, Reporting and recordkeeping requirements, Vessels.

■ Accordingly, the interim rule adding 33 CFR part 104 and amending 33 CFR parts 160 and 165, and 46 CFR parts 2, 31, 71, 91, 115, 126, and 176 that was published at 68 FR 39292 on July 1, 2003, and amended at 68 FR 41915 on July 16, 2003, is adopted as a final rule with the following changes:

**33 CFR Chapter I**

## PART 104—MARITIME SECURITY: VESSELS

■ 1. The authority citation for part 104 continues to read as follows:

**Authority:** 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

■ 2. Revise the heading to part 104 to read as shown above.

■ 3. In § 104.105—

■ a. Revise paragraphs (a)(1) through (a)(10);

■ b. Add new paragraph (a)(11); and

■ c. Revise paragraph (c) to read as follows:

**§ 104.105 Applicability.**

(a) * * *

(1) Mobile Offshore Drilling Unit (MODU), cargo, or passenger vessel subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI;

(2) Foreign cargo vessel greater than 100 gross register tons;

(3) Self-propelled U.S. cargo vessel greater than 100 gross register tons subject to 46 CFR subchapter I, except commercial fishing vessels inspected under 46 CFR part 105;

(4) Vessel subject to 46 CFR chapter I, subchapter L;

(5) Passenger vessel subject to 46 CFR chapter I, subchapter H;

(6) Passenger vessel certificated to carry more than 150 passengers;

(7) Other passenger vessel carrying more than 12 passengers, including at least one passenger-for-hire, that is engaged on an international voyage;

(8) Barge subject to 46 CFR chapter I, subchapters D or O;

(9) Barge subject to 46 CFR chapter I, subchapter I, that carries Certain Dangerous Cargoes in bulk, or that is engaged on an international voyage;

(10) Tankship subject to 46 CFR chapter I, subchapters D or O; and

(11) Towing vessel greater than eight meters in registered length that is engaged in towing a barge or barges subject to this part, except a towing vessel that—

(i) Temporarily assists another vessel engaged in towing a barge or barges subject to this part;

(ii) Shifts a barge or barges subject to this part at a facility or within a fleeting facility;

(iii) Assists sections of a tow through a lock; or

(iv) Provides emergency assistance.

* * * * *

(c) Foreign Vessels that have on board a valid International Ship Security

Certificate that certifies that the verifications required by part A, Section 19.1, of the International Ship and Port Facility Security (ISPS) Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed will be deemed in compliance with this part, except for §§ 104.240, 104.255, 104.292, and 104.295, as appropriate. This includes ensuring that the vessel meets the applicable requirements of SOLAS Chapter XI–2 (Incorporated by reference, see § 101.115 of this subchapter) and the ISPS Code, part A, having taken into account the relevant provisions of the ISPS Code, part B, and that the vessel is provided with an approved security plan.

* * * * *

■ 4. Revise § 104.110 to read as follows:

**§ 104.110 Exemptions.**

(a) This part does not apply to warships, naval auxiliaries, or other vessels owned or operated by a government and used only on government non-commercial service.

(b) A vessel is not subject to this part while the vessel is laid up, dismantled, or otherwise out of commission.

■ 5. Revise § 104.115 to read as follows:

**§ 104.115 Compliance dates.**

(a) On July 1, 2004, and thereafter, vessel owners or operators must ensure their vessels are operating in compliance with this part.

(b) On or before December 31, 2003, vessel owners or operators not subject to paragraph (c)(1) of this section must submit to the Commanding Officer, Marine Safety Center, for each vessel—

(1) The Vessel Security Plan described in subpart D of this part for review and approval; or

(2) If intending to operate under an approved Alternative Security Program, a letter signed by the vessel owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(c) On July 1, 2004, and thereafter, owners or operators of foreign vessels must comply with the following—

(1) Vessels subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI, must carry on board a valid International Ship Security Certificate that certifies that the verifications required by part A, Section 19.1, of the International Ship and Port Facility Security (ISPS) Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed. This includes ensuring that the vessel meets the applicable requirements of SOLAS Chapter XI–2 (Incorporated by reference, see § 101.115 of this chapter) and the ISPS Code, part A, having taken into account the relevant provisions of the ISPS Code, part B, and that the vessel is provided with an approved security plan.

(2) Vessels not subject to SOLAS Chapter XI, may comply with this part through an Alternative Security Program or a bilateral arrangement approved by the Coast Guard. If not complying with an approved Alternative Security Program or bilateral arrangement, these vessels must meet the requirements of paragraph (b) of this section.

■ 6. In § 104.120—

■ a. Revise paragraph (a) introductory text to read as set out below;

■ b. In paragraph (a)(3), after the words ''a copy of the Alternative Security Program the vessel is using'', add the words '', including a vessel specific security assessment report generated under the Alternative Security Program, as specified in § 101.120(b)(3) of this subchapter,''; and

■ c. Revise paragraph (a)(4) to read as follows:

**§ 104.120 Compliance documentation.**

(a) Each vessel owner or operator subject to this part must ensure, on or before July 1, 2004, that copies of the following documents are carried on board the vessel and are made available to the Coast Guard upon request:

* * * * *

(4) For foreign vessels, subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI, a valid International Ship Security Certificate (ISSC) that attests to the vessel's compliance with SOLAS Chapter XI–2 and the ISPS Code, part A (Incorporated by reference, see § 101.115 of this subchapter) and is issued in accordance with the ISPS Code, part A, section 19. As stated in Section 9.4 of the ISPS Code, part A requires that, in order for the ISSC to be issued, the provisions of part B of the ISPS Code need to be taken into account.

* * * * *

■ 7. Revise § 104.125 to read as follows:

**§ 104.125 Noncompliance.**

When a vessel must temporarily deviate from the requirements of this part, the vessel owner or operator must notify the cognizant COTP, and either suspend operations or request and receive permission from the COTP to continue operating.

■ 8. Revise § 104.140(b) to read as follows:

**§ 104.140 Alternative Security Programs.**

* * * * *

(b) The vessel is not subject to the International Convention for Safety of Life at Sea, 1974; and

* * * * *

■ 9. In § 104.200—

■ a. Revise paragraph (b)(6) to read as set out below; and

■ b. In paragraph (b)(14)(i), at the end of the word ''contractor'', add the letter ''s''.

**§ 104.200 Owner or operator.**

* * * * *

(b) * * *

(6) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility of visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with facility operators in advance of a vessel's arrival. Vessel owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations in coordinating such leave. The text of these treaties can be found on the U.S. Department of State's Web site at *http://www.state.gov/s/l/24224.htm;*

* * * * *

**§ 104.205 [Amended]**

■ 10. In § 104.205(b)(1), after the words ''inform the Coast Guard'', add the words ''via the NRC'' and remove the text ''1st-nrcinfo@comdt.uscg.mil'' and add, in its place, the text ''lst-nrcinfo@comdt.uscg.mil''.

**§ 104.210 [Amended]**

■ 11. In § 104.210(a)(3), after the words ''owner or operator's organization,'' add the words ''including the duties of a Vessel Security Officer,''.

**§ 104.215 [Amended]**

■ 12. In § 104.215—

■ a. In paragraph (a)(2), after the words ''the VSO must be'', add the words ''the Master or''; and

■ b. In paragraph (a)(3), after the words ''For unmanned vessels,'' add the words ''the VSO must be an employee of the company, and'' and remove the words ''more one than'' and add, in their place, the words ''more than''.

**§ 104.225 [Amended]**

■ 13. In § 104.225, in the introductory paragraph, after the words ''in the following'' add the words '', as appropriate''.

■ 14. In § 104.230—

■ a. Revise paragraph (a) to read as set out below;

■ b. In paragraph (b)(4), after the word ''week'', add the word ''from''; and

■ c. Add paragraph (b)(5) to read as follows:

**§ 104.230 Drill and exercise requirements.**

(a) *General.* (1) Drills and exercises must test the proficiency of vessel personnel in assigned security duties at all Maritime Security (MARSEC) Levels and the effective implementation of the Vessel Security Plan (VSP). They must enable the Vessel Security Officer (VSO) to identify any related security deficiencies that need to be addressed.

(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the Vessel Security Plan as the result of an increase in the MARSEC Level, provided the vessel reports attainment to the cognizant COTP.

(b) * * *

(5) Not withstanding paragraph (b)(4) of this section, vessels not subject to SOLAS may conduct drills within 1 week from whenever the percentage of vessel personnel with no prior participation in a vessel security drill on a vessel of similar design and owned or operated by the same company exceeds 25 percent.

* * * * *

**§ 104.235 [Amended]**

■ 15. In § 104.235—

■ a. In paragraph (b)(1), remove the words ''each security training session'' and add, in their place, the words ''training under § 104.225''; and

■ b. In paragraph (b)(8), after the words ''letter certified by'', add the words ''the Company Security Officer or''.

■ 16. In § 104.240—

■ a. In paragraph (a), after the words ''prior to entering a port'', add the words ''or visiting an Outer Continental Shelf (OCS) facility'' and, after the words ''in effect for the port'', add the words ''or the OCS facility'';

■ b. In paragraph (b)(2), remove the word ''and'';

■ c. In paragraph (b)(3), at the end of the paragraph, remove the period and add, in its place, the text ''; and''; and

■ d. Add paragraph (b)(4) to read as follows:

**§ 104.240 Maritime Security (MARSEC) Level coordination and implementation.**

* * * * *

(b) * * *

(4) If a higher MARSEC Level is set for the OCS facility with which the vessel is interfacing or is about to visit, the vessel complies, without undue delay, with all measures specified in the VSP for compliance with that higher MARSEC Level.

* * * * *

■ 17. In § 104.255—

■ a. Revise paragraphs (b)(2), (c), and (d) to read as set out below; and

■ b. In paragraph (g), after the words ''vessel-to-vessel'' add the word ''activity'':

**§ 104.255 Declaration of Security (DoS).**

* * * * *

(b) * * *

(2) For a vessel engaging in a vessel-to-vessel activity, prior to the activity, the respective Masters, VSOs, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, VSOs, or designated representatives must sign the written DoS.

(c) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, VSOs, or designated representatives must sign the written DoS.

(d) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period the vessel is at the facility. Upon the vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective FSO and Master, VSO, or designated representatives must sign the written DoS.

* * * * *

**§ 104.265 [Amended]**

■ 18. In § 104.265—

■ a. In paragraph (b) introductory text, after the words ''ensure that'', add the words ''the following are specified'';

■ b. In paragraph (b)(1), remove the words ''to prevent unauthorized access'';

■ c. In paragraph (b)(3), remove the words ''are established'';

■ d. In paragraph (c)(5), remove the word ''seafarer's'' and add, in its place, the word ''seafarers' '':

■ e. In paragraph (e)(1), after the word ''Vessel Security Plan (VSP)'' add the words '', except for government-owned vehicles on official business when government personnel present identification credentials for entry'';

■ f. In paragraph (e)(9), remove the words ''required to engage in or be''; and

■ g. In paragraph (f)(1), after the word ''approved VSP'', add the words '', except for government-owned vehicles on official business when government personnel present identification credentials for entry''.

**§ 104.275 [Amended]**

■ 19. In § 104.275—

■ a. In paragraph (a) introductory text, after the word ''facility'', add the words ''or another vessel'';

■ b. In paragraph (a)(4), at the end of the paragraph, add the word ''and'';

■ c. In paragraph (a)(5), remove the word ''Coordinate'', and add, in its place, the words ''When there are regular or repeated cargo operations with the same shipper, coordinate'' and, at the end of the paragraph, remove the text ''; and'' and add, in its place, a period;

■ d. Remove paragraph (a)(6);

■ e. In paragraph (b)(1), remove the word ''Routinely'', add the words ''Unless unsafe to do so, routinely'' and, after the words ''cargo handling'', add the words ''for evidence of tampering'';

■ f. In paragraph (c)(1), after the words ''cargo spaces'' add the words ''for evidence of tampering'';

■ g. In paragraph (c)(5), remove the words ''of the use of scanning/detection equipment, mechanical devices, or canines'' and add, in their place, the words ''and intensity of visual and physical inspections''; and

■ h. In paragraph (d)(2), remove the words ''and facilities'' and add, in their place, the words '', facilities, and other vessels''.

**§ 104.285 [Amended]**

■ 20. In § 104.285—

■ a. In paragraph (a)(1), after the word ''patrols'', add a comma and remove the word ''and'';

■ b. In paragraph (b)(4), remove the word ''continually'' and add, in its place, the word ''continuously''; and

■ c. In paragraph (c)(5), remove the word ''or'' and add, in its place, the word ''and''.

■ 21. In § 104.292—

■ a. Redesignate paragraphs (d) and (e) as paragraphs (e) and (f), respectively;

■ b. In newly redesignated paragraph (e)(3), after the words ''requirements in § 104.265(e)(3)'', add the words ''and (f)(1)'';

■ c. In newly redesignated paragraph (f), after the words ''requirements in § 104.265(e)(3)'', add the words ''and § 104.265(g)(1)''; and

■ d. Add new paragraph (d) to read as follows:

**§ 104.292 Additional requirements—passenger vessels and ferries.**

* * * * *

(d) Owners and operators of passenger vessels and ferries covered by this part that use public access facilities, as that term is defined in § 101.105 of this subchapter, must address security measures for the interface of the vessel and the public access facility, in accordance with the appropriate Area Maritime Security Plan.

* * * * *

**§ 104.297 [Amended]**

■ 22. In § 104.297(c), remove the words ''prior to July 1, 2004'' and add, in their place, the words ''on or before July 1, 2004''.

**§ 104.300 [Amended]**

■ 23. In § 104.300(d)(8), after the words ''Vessel-to-vessel'', add the word ''activity''.

**§ 104.305 [Amended]**

■ 24. In § 104.305—

■ a. In the introductory text to paragraphs (d)(3), (d)(4), and (d)(5), after the word ''VSA'', add the word ''report'';

■ b. In § 104.305(d)(3)(iv) after the words ''dangerous goods'' remove the word ''or'' and replace with the word ''and''; and

■ c. Redesignate paragraph (d)(6) as paragraph (e) and, in the second sentence, after the words ''The VSA'', add the words '', the VSA report,''.

■ 25. Add § 104.310(c) to read as follows:

**§ 104.310 Submission requirements.**

* * * * *

(c) The VSA must be reviewed and revalidated, and the VSA report must be updated, each time the VSP is submitted for reapproval or revisions.

**§ 104.400 [Amended]**

■ 26. In § 104.400—

■ a. In paragraph (a)(2), after the words ''Must be written in English'' add the words '', although a translation of the VSP in the working language of vessel personnel may also be developed''.

■ b. Revise paragraph (b) to read as follows:

**§ 104.400 General.**

* * * * *

(b) The VSP must be submitted to the Commanding Officer, Marine Safety Center (MSC) 400 Seventh Street, SW., Room 6302, Nassif Building, Washington, DC 20590–0001, in a written or electronic format. Information for submitting the VSP electronically can be found at *http://www.uscg.mil/HQ/MSC.* Owners or operators of foreign flag vessels that are subject to SOLAS Chapter XI must comply with this part by carrying on board a valid International Ship Security Certificate that certifies that the verifications required by Section 19.1 of part A of the ISPS Code (Incorporated by reference, *see* § 101.115 of this subchapter) have been completed. As stated in Section 9.4 of the ISPS Code, part A requires that, in order for the ISSC to be issued, the provisions of part B of the ISPS Code need to be taken into account.

* * * * *

■ 27. In § 104.410—

■ a. Revise the introductory text for paragraph (a) to read as set out below;

■ b. In paragraph (a)(1), after the words ''Vessel Security Plan (VSP)'', add the words '', in English,'';

■ c. Revise paragraphs (a)(2) and (b) to read as set out below;

■ d. In paragraph (c)(1), remove the words '', or'' and add, in their place, a semicolon;

■ e. Redesignate paragraph (c)(2) as paragraph (c)(3);

■ f. Add new paragraph (c)(2) to read as follows:

**§ 104.410 Submission and approval.**

(a) In accordance with § 104.115, on or before December 31, 2003, each vessel owner or operator must either:

* * * * *

(2) If intending to operate under an Approved Security Program, a letter signed by the vessel owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) Owners or operators of vessels not in service on or before December 31, 2003, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations or by December 31, 2003, whichever is later.

(c) * * *

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

* * * * *

■ 28. In § 104.415—

■ a. In paragraph (a)(1), remove the text ''MSC'' and, add in its place, the words ''Marine Safety Center (MSC)'';

■ b. In paragraph (a)(2), remove the words ''Marine Safety Center'' and the words ''Marine Safety Center (MSC)'' and add, in their place, the text ''MSC''; and

■ c. Redesignate paragraph (a)(3) as (a)(4) and add new paragraph (a)(3) to read as follows:

**§ 104.415 Amendment and audit.**

(a) * * *

(3) Nothing in this section should be construed as limiting the vessel owner or operator from the timely implementation of such additional security measures not enumerated in the approved VSP as necessary to address exigent security situations. In such cases, the owner or operator must notify the MSC by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

* * * * *

**46 CFR Chapter I**

## PART 2—VESSEL INSPECTIONS

■ 29. The authority citation for part 2 continues to read as follows:

**Authority:** 33 U.S.C. 1903; 43 U.S.C. 1333; 46 U.S.C. 3103, 3205, 3306, 3307, 3703; 46 U.S.C. Chapter 701; Executive Order 12234, 45 FR 58801, 3 CFR, 1980 Comp., p. 277; Department of Homeland Security Delegation No. 0170.1; subpart 2.45 also issued under the authority of Act Dec. 27, 1950, Ch. 1155, secs. 1, 2, 64 Stat. 1120 (see 46 U.S.C. App. Note prec. 1).

■ 30. Add § 2.01–25(a)(2)(viii) to read as follows:

**§ 2.01–25 International Convention for Safety of Life at Sea, 1974.**

(a) * * *

(2) * * *

(viii) International Ship Security Certificate (ISSC).

* * * * *

Dated: October 8, 2003.

**Thomas H. Collins,**

*Admiral, U.S. Coast Guard Commandant.*

[FR Doc. 03–26347 Filed 10–17–03; 8:45 am]

**BILLING CODE 4910–15–P**

---

## DEPARTMENT OF HOMELAND SECURITY

### Coast Guard

### 33 CFR Part 105

**[USCG–2003–14732]**

**RIN 1625–AA43**

### Facility Security

**AGENCY:** Coast Guard, DHS.

**ACTION:** Final rule.

**SUMMARY:** This final rule adopts, with changes, the temporary interim rule published on July 1, 2003, that provides security measures for certain facilities in U.S. ports. It also requires owners or operators of facilities to designate security officers for facilities, develop security plans based on security