§ 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

assessments and surveys, implement security measures specific to the facility's operations, 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 21, 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–2003–14732 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 Gregory Purvis (G–MPS–1), U.S. Coast Guard by telephone 202–267–1072 or by electronic mail *gpurvis@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 ''Facility Security'' in the **Federal Register** (68 FR 39315). 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 41916).

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 ''Facility 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 rules. 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 128, Security of Passenger Terminals, currently exists but applies only to cruise ship terminals. Until July 2004, 33 CFR part 128 will remain in effect. Facilities that were required to comply with part 128 must now also meet the requirements of this part, including § 105.290, titled ''Additional requirements—cruise ship terminals.'' The requirements in § 105.290 generally capture the existing requirements in part 128 that are specific for cruise ship terminals and capture additional detail to comply with the requirements of SOLAS Chapter XI–2 and the 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 105.

One commenter stated the public access area was a very well thought out concept. Another commenter stated that the thresholds and exempted facilities specified in § 105.105 should remain as written.

One commenter requested that § 105.105(a)(2) be revised, stating that the security requirements of facilities should be based on the terminal's size and capacity alone, rather than on the number of passengers a vessel is certificated to carry.

While a terminal's size or capacity is a way to determine applicability, we chose to focus on vessel interface and cargo handling activities because this method is consistent with the conceptual applicability standards employed internationally. When we focused on vessel-to-facility interfaces, our risk assessment showed that vessels certificated to carry over 150 passengers, and the facilities servicing them, may be involved in a transportation security incident.

Two commenters requested clarification on our reference to International Convention for Safety of Life at Sea, 1974, (SOLAS) and facility applicability. One commenter stated that because the applicability of the various chapters of SOLAS is not consistent, it is necessary to specify particular chapters in SOLAS to define the applicability of this regulation to U.S. flag vessels. The commenter

requested that we limit the reference to SOLAS in § 105.105(a)(3) to ''SOLAS Chapter XI–2.'' Another commenter stated that it is not clear whether the words ''greater than 100 gross registered tons'' applied to SOLAS vessels as well as to vessels that are subject to 33 CFR subchapter I.

We agree that the general reference to SOLAS is broad and could encompass more vessels than necessary. We have amended the applicability reference to read ''SOLAS Chapter XI'' because subchapter H addresses those requirements in SOLAS Chapter XI. Also, we have amended § 105.105(a) to apply the term ''greater than 100 gross registered tons'' to facilities that receive vessels subject only to subchapter I. We did not include references to foreign or U.S. ownership in the applicability paragraphs because it is duplicative of the existing language.

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.

Five commenters addressed the applicability of the regulations with respect to facilities and the boundaries of the Coast Guard jurisdiction relative to that of other Federal agencies. Four commenters advocated a ''firm line of demarcation'' limiting the Coast Guard authority to the ''dock,'' because as the rule is now written, a facility may still be left to wonder which Federal agency or department might have jurisdiction over it when it comes to facility security. One commenter suggested that the Coast Guard jurisdiction should not extend beyond ''the first continuous access control boundary shore side of the designated waterfront facility.''

Section 102 of the MTSA requires the Secretary of the Department in which the Coast Guard is operating to prescribe certain security requirements for facilities. The Secretary has delegated that authority to the Coast Guard. Therefore, the Coast Guard is not only authorized, but also required under the MTSA, to regulate beyond the ''dock.''

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.

Six commenters stated that the term ''fleeting facility'' in § 105.105(a)(4) is more general than the definition of a ''barge fleeting facility'' in § 101.105. The commenters pointed out that temporary staging areas of barges, or those areas for the breaking and making of tows provided by the U.S. Army Corps of Engineers, are not included in the definition of ''barge fleeting facility'' because they are not ''commercial fleeting areas.'' The commenters suggested that these areas be included in AMS Plans.

We agree with the commenters and are amending § 105.105(a)(4) to make it consistent with the definition stated in § 101.105 for ''barge fleeting facility.'' This new language can be found in § 105.105(a)(6). With regards to barge fleeting areas that are provided by the U.S. Army Corps of Engineers, in accordance with § 105.105(b), those facilities that are not subject to part 105 will be covered by parts 101 through 103 of this subchapter and will be included in the AMS Plan for the COTP zone in which the facility is located.

Three commenters disagreed with including all barge fleeting facilities that handle barges carrying hazardous material in the security requirements. The commenters stated that the security requirements are an undue burden on industry because the fleeting facilities are remote and routinely inaccessible by shore.

We developed the fleeting facility security requirements because these facilities may, if they fleet hazardous barges, be involved in a transportation security incident. Remoteness or inaccessibility of fleeting facilities will be factors to consider during the Facility Security Assessment and will be key in determining the security measures to be implemented.

One commenter noted that § 105.105(a)(4) does not apply to barges in a gas-free state, and suggested that we amend this paragraph to read, ''whether loaded, unloaded, or gas-free.''

Section 105.105(a)(4) applies to those barges that are actually loaded with cargoes regulated under 46 CFR subchapter D or O, not those that are gas-free. Barges that are gas-free are unlikely to be involved in a transportation security incident.

Three commenters recommended that we amend § 105.105(c)(3) to clarify the applicability of facilities that support the production, exploration, or development, of oil and natural gas.

We agree with the commenters that the exemptions in § 105.105(c)(3) are confusing and are amending this section for clarity.

Two commenters requested exemptions for ''facilities that handle certain fertilizers,'' stating that they do not pose risks to human health or the

environment from a transportation security perspective. The commenters requested that we exempt facilities that handle only certain non-hazardous fertilizers from the requirements of part 105, stating that these facilities are not likely to be involved in a transportation security incident.

Our risk assessment determined that facilities that receive vessels on international voyages, including those that carry non-hazardous fertilizers, may be involved in a transportation security incident. We are not, therefore, amending the applicability for facilities in part 105 to exempt these facilities. The facility owner or operator may apply to the Commandant (G-MP) for a waiver as specified in § 105.130. Because a Facility Security Plan is based on the results of the Facility Security Assessment, the security measures implemented will be tailored to the operations of the facility. Those security measures will be appropriate for that facility, but will differ from the measures implemented at a facility that handles dangerous goods or hazardous substances.

One commenter stated that we needed to clarify how the regulations apply to facilities in ''caretaker status.''

Facilities operating with ''caretaker status'' as defined in 33 CFR 154.105, that are not engaged in any of the activities regulated under part 105, will be covered under parts 101 through 103. Facilities in ''caretaker status'' engaging in or intending to engage in any of the activities regulated under § 105.105 must comply with part 105 by conducting a Facility Security Assessment and, 60 days prior to beginning operations, submitting a Facility Security Plan to the local COTP for approval. In such situations, the ''caretaker'' is the ''owner or operator'' as that term is defined in the regulations.

Six commenters stated that part 105 should not apply to marinas that receive a small number of passenger vessels certificated to carry more than 150 passengers or to ''mixed-use or special-use facilities which might accept or provide dock space to a single vessel'' because the impact on local business in the facility could be substantial. Two commenters stated that private and public riverbanks should not be required to comply with part 105 because ''there is no one to complete a Declaration of Security with, and no way to secure the area, before the vessel arrives.'' Two commenters stated that facilities that are ''100 percent public access'' should not be required to comply with part 105 because these types of facilities are ''vitally important to the local economy, as well as to the host municipalities.'' This commenter also stated that vessels certificated to carry more than 150 passengers frequently embark guests at private, residential docks and small private marinas for special events such as weddings and anniversaries and may visit such a dock only once.

We agree that the applicability of part 105 to facilities that have minimal infrastructure, but are capable of receiving passenger vessels, is unclear. Therefore, in the final rule for part 101, we added a definition for a ''public access facility'' to mean a facility approved by the cognizant COTP with public access that is primarily used for purposes such as recreation or entertainment and not for receiving vessels subject to part 104. By definition, a public access facility has minimal infrastructure for servicing vessels subject to part 104 but may receive ferries and passenger vessels other than cruise ships, ferries certificated to carry vehicles, or passenger vessels subject to SOLAS. Minimal infrastructure would include, for example, bollards, docks, and ticket booths, but would not include, for example, permanent structures that contain passenger waiting areas or concessions. We have not allowed public access facilities to be designated if they receive vessels such as cargo vessels because such cargo-handling operations require additional security measures that public access facilities would not have. We amended part 105 to exclude these public access facilities, subject to COTP approval, from the requirements of part 105. We believe this construct does not reduce security because the facility owner or operator or entity with operational control over these types of public access facilities still has obligations for security that will be detailed in the AMS Plan, based on the AMS Assessment. Additionally, Vessel Security Plans must address security measures for using the public access facility. This exemption does not affect existing COTP authority to require the implementation of additional security measures to deal with specific security concerns. We have also amended § 103.505, to add public access facilities to the list of elements that must be addressed within the AMS Plan.

We received 26 comments dealing with the definition of ''facility.'' One commenter asked whether a facility that is inside a port that handles cargo or containers, but does not have direct water access, is covered under the definition of facility. Another commenter recommended that the definition specify that facilities without water access and that do not receive vessels be exempt from the requirements. One commenter asked whether small facilities located inland on a river would be subject to part 105 if they receive vessels greater than 100 gross registered tons on international voyages. One commenter asked whether a company that receives refined products via pipeline from a dock facility that the company does not own qualifies as a regulated facility. One commenter asked whether part 105 applies to facilities at which vessels do not originate or terminate voyages. Two commenters stated that the word ''adjacent'' in the definition should be changed to read ''immediately adjacent'' to the ''navigable waters.'' One commenter suggested that, in the definition, the word ''adjacent'' be defined in terms of a physical distance from the shore and the terms ''on, in, or under'' and ''waters subject to the jurisdiction of the U.S.'' be clarified. Two commenters understand the definition of ''facility'' to possibly include overhead power cables, underwater pipe crossings, conveyors, communications conduits crossing under or over the water, or a riverbank. One commenter asked for a blanket exemption for electric and gas utilities. One commenter suggested rewriting the applicability of ''facilities'' in plain language or, alternatively, providing an accompanying guidance document to help owner and operators determine whether their facilities are subject to these regulations. One commenter asked us to clarify which facilities might ''qualify'' for future regulation and asked us to undertake a comprehensive review of security program gaps and overlaps, in coordination with DHS. One commenter stated that a facility that receives only vessels in ''lay up'' or for repairs should not be required to comply with part 105.

We recognize that the definition of ''facility'' in § 101.105 is broad, and we purposefully used this definition to be consistent with existing U.S. statutes regarding maritime security. A facility within an area that is a marine transportation-related terminal or that receives vessels over 100 gross tons on international voyages is regulated under § 105.105. All other facilities in an area not directly regulated under § 105.105, such as some adjacent facilities and utility companies, are covered under parts 101 through 103. If the COTP determines that a facility with no direct water access may pose a risk to the area, the facility owner or operator may be required to implement security

measures under existing COTP authority. With regard to facilities that receive only vessels in ''lay up'' or for repairs, we amended the regulations to define, using the definition of a general shipyard facility from 46 CFR 298.2, and exempt general shipyard facilities from the requirements of part 105 unless the facility is subject to 33 CFR parts 126, 127, or 154 or provides any other service beyond those services defined in § 101.105 to any vessel subject to part 104. In a similar manner, in part 105, we are also exempting facilities that receive vessels certificated to carry more than 150 passengers if those vessels do not carry passengers while at the facility nor embark or disembark passengers from the facility. We exempted facilities that receive vessels for lay-up, dismantling, or placing out of commission to be consistent with the other changes we have discussed above. The facilities listed in the amended § 105.105 as exceptions and § 105.110 as exemptions will be covered by the AMS Plan, and we intend to issue further guidance on addressing these facilities in the AMS Plan. Finally, while not in ''plain language'' format, we have attempted to make these regulations as clear as possible. We have created Small Business Compliance Guides, which should help facility owners and operators determine if their facilities are subject to these regulations. These Guides are available where listed in the ''Assistance for Small Entities'' section of this final rule.

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.

After further review of the rules, we are amending the dates of compliance in § 105.115(a) and (b), § 105.120 introductory text, and § 105.410(a) to align with the MTSA and the International Ship and Port Facility Security Code (ISPS Code) compliance dates. For example, we are changing the deadline in § 105.115(a) for submitting a Facility Security Plan from December 29, 2003, to December 31, 2003.

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.

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.

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.

After further review of parts 101 and 104–106, we have 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.

One commenter stated that facilities should be permitted to use equivalent security measures because facilities vary greatly in their design and security risk profile.

We agree and have provided facilities the opportunity to apply for approval of equivalent security measures in § 105.135.

Subpart B—Facility Security Requirements

This subpart describes the responsibilities of the facility owner or operator and personnel relative to facility 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 types of facilities.

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 identified 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, and the Coast Guard will review these records during periodic inspections.

One commenter stated that it is appropriate for Federal, State, and local authorities to assume responsibility for terminal security, and that there must be a responsible party for the terminal at all times whether a vessel is there or not.

Section 105.200(a) states that the owner or operator of the facility must ensure that the facility operates in compliance with the requirements of this part. Therefore, the owner or operator is responsible for terminal security at all times whether or not a vessel is at the facility.

Five commenters stated that the requirement of § 105.200(b)(2), which compels Facility Security Officers to implement security measures in response to MARSEC Levels within 12 hours of notification would be problematic, especially for facilities with limited manpower, and during weekends, or nights.

We disagree with the commenters and believe that it is well within reason to expect that Facility Security Officers can implement the necessary security measures changes within 12 hours.

Two commenters recommended that the word ''adequate'' be deleted from § 105.200(b)(6) because the commenter believes that the owners' or operators' definition of ''adequate'' might not be the same as intended in the regulations.

The use of the word ''adequate'' throughout the regulations emphasizes that minimal coordination of security issues may not be sufficient and allows for differences in individual circumstances.

One commenter recommended that facility owners or operators should limit access to vessels moored at the facility to those individuals and organizations that conduct business with the vessel, contending that the word ''visitor'' may have too broad a connotation.

The regulations provide flexibility to define who can have access to a facility. The Facility Security Plan must contain security measures for access control and can limit access to those individuals and organizations that conduct business with the vessel. We do specify that a facility must ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility for representatives of seafarers' welfare and labor organizations.

One commenter suggested adding a provision that would allow unimpeded access for passengers to board charterboats at facilities regulated under part 105, stating that the ''extraordinary measures'' required to ensure facility security could hamper public entrance to these facilities.

A facility owner or operator must coordinate access to the facility with vessel personnel under § 105.200(b)(7); however, that owner or operator is also required to implement security measures that include access control. We did not allow any group of vessel passengers or personnel unimpeded access to a facility regulated under this subchapter because it would undermine the purpose of access control. A facility owner or operator may impede passengers' access to charterboats if he or she perceives that these passengers pose a risk, are at risk, or if such passage is not in compliance with the facility's security plan.

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 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 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.

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.

Four commenters stated that any future interim rules should not apply to certain waterfront areas, such as seafarers' welfare centers and clubs, and that these areas should not be considered facilities subject to the regulations under part 105.

Seafarers' welfare centers and clubs are not specifically regulated under part 105 unless these facilities are contained within a marine transportation-related facility. Any future rulemakings regarding these types of centers or clubs would be subject to notice and comment.

One commenter requested that we amend § 105.200(b)(9) to clarify that owners or operators must report ''transportation'' security incidents because the word ''transportation'' is missing.

We agree with the commenter and have amended the section accordingly. This language is now found in § 105.200(b)(10).

Five commenters supported the Coast Guard in not specifically defining training methods. Another commenter agrees with the Coast Guard's position that the owner or operator may certify that the personnel with security responsibilities are capable of performing the required functions based upon the competencies listed in the regulations. Two commenters stated that formal security training for Facility Security Officers and personnel with security related duties become mandatory as soon as possible. One commenter stated that they were concerned with the lack of formal training for Facility Security Officers.

As we explained in the temporary interim rule (68 FR 39263) (part 101), there are no approved courses for facility personnel and, therefore, we intend to allow Facility Security Officers to certify that personnel holding a security position have received the training required to fulfill their security duties. Section 109 of the MTSA required the Secretary of Transportation to develop standards and curricula for the education, training, and certification of maritime security personnel, including Facility Security Officers. The Secretary delegated that authority to the Maritime Administration (MARAD). MARAD has developed model training standards and curricula for maritime security personnel, including Facility Security Officers. In addition, MARAD intends to develop course approval and certification requirements in the near future.

Three commenters stated that it would be difficult for smaller companies to meet the qualification requirements for Facility Security Officers that are set out in § 105.205.

We recognize that some companies will find it harder than others to locate individuals who are qualified to serve as Facility Security Officers. We believe there is flexibility in the structure of our requirements, and therefore these requirements are able to take this into account. We allow Facility Security Officers to have general knowledge, which they may acquire through training or through equivalent job experience. Formal training is not a prerequisite in the designation of a Facility Security Officer. We also allow an individual to serve as a Facility Security Officer on a collateral-duty basis, to serve as the Facility Security Officer for multiple facilities, and to delegate duties, all of which make it easier for companies to identify and designate qualified Facility Security Officers.

Fifteen commenters asked that the Coast Guard re-examine the requirement that if a Facility Security Officer serves more than one facility, those facilities must be no further than 50 miles apart. The commenters argued that companies with multiple facilities should be able to assign Facility Security Officer delegations, regardless of distance between facilities, especially since this section allows the Facility Security Officer to delegate security duties to other personnel, so long as he or she retains final responsibility for these duties. Four of these commenters did not support the limitation on Facility Security Officers from serving facilities in different COTP zones, even if the facilities are within 50 miles of each other. One commenter stated that many facilities that are not co-located may be managed as multiple site complexes using shared operational and administrative resources, and that, as such, they should have one Facility Security Officer assigned to them regardless of the distance between them.

We believe these commenters misinterpreted § 105.205(a)(2). There is no requirement that the Facility Security Officer must be situated within any particular distance of the facilities for which he or she serves. Section 105.205(a)(2) pertains to the maximum distance between the individual facilities that can be served by a single Facility Security Officer. We determined that a distance of 50 miles between facilities within a single COTP zone was appropriate for several reasons. During our initial public meetings we received comments from many small facility operators who have numerous similarly designed, equipped and operated facilities in proximity to each other. They believed that a single Facility Security Officer could adequately meet the responsibilities set out in § 105.205(c) in situations like this. The 50-mile distance requirement was determined because facilities sharing a similar design, equipment, and operations would often share other similar characteristics such as geography, infrastructure, proximity to population centers, and common emergency response and crisis management authorities. In addition to the 50-mile limit, we require all single Facility-Security-Officer-served-facilities to be within a single COTP zone because the COTP is the Facility Security Plan approving authority, and the COTP, as Federal Maritime Security Coordinator, is the Federal official charged with communicating the MARSEC Levels to the Facility Security Officer. We have not specified where the designated Facility Security Officer must be in proximity to the facilities he or she serves. However, it is our opinion that in order to effectively carry out the duties and responsibilities specified in § 105.205(c), the Facility Security Officer should be able to easily make on-site facility visits of sufficient frequency and scope so as to be able to effectively monitor compliance with the requirements established in 33 CFR part 105.

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 106.210(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 stated that the Facility Security Officer should be allowed to assign the day-to-day security activities to other personnel.

The regulations, allow for the Facility Security Officers to assign security duties to other facility personnel under § 105.205(a)(3).

After further review of § 105.205, we are amending § 105.205(c)(11) to clarify that the responsibilities of the Facility Security Officer includes the execution of any required Declarations of Security with the Masters, Vessel Security Officers, or their designated representatives.

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.

One commenter stated that crowd management and control techniques, under § 105.210(e), should not be required of facility personnel with security duties, stating that this function is solely a responsibility of public responders.

We believe that crowd management and control techniques may be appropriate for facility security personnel with certain security duties. The overall security and safe operation of a facility rests with the owner or operator of that facility. It is not outside the realm of facility personnel's duties to consider security and their role in minimizing risk, including crowd management and control techniques.

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.

One commenter suggested exempting ferry terminals from § 105.210(l) concerning methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores because ''it is not applicable.''

We disagree that all ferry terminals should be exempted, as this comment appears to presuppose that portions of the regulations are not applicable to all ferry terminals. We determined that facilities that receive vessels certificated to carry more than 150 passengers are at risk of being involved in a transportation security incident and are regulated under § 105.105.

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 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 a facility 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.

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

Eleven commenters requested clarification on drills and exercises. One commenter suggested that an exercise be defined as a tabletop exercise, while a drill be a one-topic, specific exercise that is one-hour in length and is easily incorporated into daily operating activities. The commenter also suggested that the frequency of exercise requirements be extended to once every three years. Additionally, two commenters requested that security drills and exercises be integrated with non-security drills and exercises. Two commenters requested that certain

facilities be allowed to deviate from the requirements in § 105.220. Two commenters stated that exercises should be a company-wide test of a company's security readiness. One commenter requested a waiver from the three drills per year requirement, based upon facility size.

We disagree that exercises should be exclusively tabletop exercises. Under § 105.220(c), exercises may be full scale or live, tabletop simulation, or seminar or combined with other appropriate exercises as stated in § 105.220(c)(2)(i–iii). Section 105.220(b) provides enough flexibility for drills to allow them to be incorporated into daily operations. We do not disagree that a drill may be accomplished in a one-hour period but believe that the length of time would actually depend on which portion of the security plan the drill is testing. Therefore, we did not constrict or prescribe a drill time-length in the regulation. We believe that annual exercises are necessary for each facility to maintain an adequate level of security readiness. These security exercises, however, may be part of a cooperative exercise program with applicable facility and vessel security plans or comprehensive port exercises as stated in § 105.220(c)(3). We agree that the exercises should be a company-wide test of a company's security readiness in its areas of operation. Additionally, any facility owner or operator may request a waiver from any of the security requirements, in light of the operating conditions of the facility, in accordance with § 105.130.

Four commenters suggested that security drills are not needed when the only option is to call ''911.''

Although calling ''911'' may test one element of the Facility Security Plan, additional drills are required to cover the other elements of the Facility Security Plan to ensure its effective implementation.

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 the vessel.

One commenter asked for a definition of ''security equipment'' and suggested using the term ''security system'' instead. The commenter also asked how much detail must be included in records of maintenance, calibration, and testing.

Depending on how a facility owner or operator decides to implement the security measures of this part, either term would be appropriate. Some may choose to install stand-alone equipment, while others may choose to have an integrated security system. We did not prescribe specific details for recordkeeping of security equipment because of the diverse possibilities of implementation. The intent of the recordkeeping requirements in § 105.225 was to keep a general log of calibration, testing, and maintenance performed.

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).

Six commenters stated that the majority of the recordkeeping requirements for facilities and OCS facilities were overly burdensome and unnecessary. One commenter suggested adding exemptions to § 105.110(b) to exempt public access areas from the recordkeeping requirements under §§ 105.225(b)(3), (b)(4), (e)(8) and (e)(9).

We disagree with the commenters. Recordkeeping serves the vital function of documenting compliance with the regulations. We also disagree that exemptions from the recordkeeping requirements are appropriate for public access areas. We note that there is no § 105.225(e).

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 security 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 ways to communicate changes in MARSEC Levels, from a timing standpoint, are via email, 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 ways. 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.

Six comments were received concerning the requirement that facilities communicate changes in MARSEC Levels to vessels. Four commenters requested that OCS facilities only notify those vessels subject to part 104 of a change in MARSEC Level, instead of notifying all vessels conducting operations with the OCS facility, vessels moored to a facility, or scheduled to arrive within 96 hours.

We disagree with the commenter. Although vessels not covered under part 104 may not be likely to be involved in a transportation security incident, they may interface with facilities that are likely to be involved in a transportation security incident. Therefore, the Coast Guard requires facilities to transmit the necessary information on MARSEC Levels to all vessels they interface with regardless of whether the vessels have their own Vessel Security Plan to ensure that security at the facilities is not compromised.

We received 15 comments on the facility owner's or operator's responsibility to communicate changes in MARSEC Levels to vessels bound for the facility. Nine commenters noted that it would be difficult and impractical for facilities to notify vessels 96 hours prior to arrival of changes in MARSEC Levels because some vessels and facilities do not have a means to provide secure communications. Three commenters stated that facilities should not be responsible for notifying vessels that have not arrived at the facility of MARSEC Level changes. In contrast, one commenter suggested that the Coast Guard amend § 101.300(a) to include a provision for facilities to notify vessels of MARSEC Level changes within 96 hours, much like that which is currently found in § 105.230(b)(1).

The intent of the regulations was to give vessel owners or operators the maximum amount of time possible to ensure the higher MARSEC Level is implemented on the vessel prior to interfacing with a facility. This ensures that the facility's security at the higher MARSEC Level is not compromised when the vessel arrives. Therefore, while it may be difficult to contact a vessel in advance of its arrival, it is imperative for the security of the facility and the vessel. Additionally, communications between the facility and the vessel do not need to be secure, as MARSEC Levels are not classified information. We have not amended § 101.300(a), as the commenter suggested, because this section is intended to regulate communication at the port level, whereas § 105.230(b)(1) is intended to regulate communication at the individual facilities within the port.

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.

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.

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 agree that the owners and operators of barge fleeting facilities have control of unmanned vessels that are moored at their facilities. As such, it is the responsibility of the facility owner or operator to ensure that the COTP is notified when compliance with a higher MARSEC Level has been implemented at the facility, including on the unmanned vessels moored at the facility.

Two commenters stated that § 105.235(b) requires an effective means of communications be in place and documented in the facility plan. One of the commenters asked if it was acceptable to communicate with the vessel through the person in charge.

Section 105.235(b) provides enough flexibility that it may be appropriate to list the person in charge, as defined in 33 CFR part 155, as a means of communication in the Facility Security Plan, provided it meets with the approval of the cognizant COTP.

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 effectively communicate with each other in order to 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.

Two commenters did not support the restriction on the Facility Security Officer from being able to delegate authority to other security personnel in periods of MARSEC Levels 2 and 3. The commenters suggested that the Coast Guard use the same language in § 105.245(b), which allows the Facility Security Officer to delegate authority to a designated representative to sign and implement a Declaration of Security at MARSEC Levels 2 and 3.

Section 105.205 allows the Facility Security Officer to delegate security duties to other facility personnel. This delegation applies to the authority of the Facility Security Officer to sign and implement a Declaration of Security at MARSEC Levels 2 and 3. In order to clarify the regulations, however, we have amended § 105.245(d) to include the language found in § 105.245(b), allowing the Facility Security Officer to delegate this authority. We have also made the same change in § 106.250(d).

Three commenters suggested that the regulation should require that the Vessel Security Officer and Facility Security Officer have verified—via e-mail, 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 interface.

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 in §§ 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 suggested that we add language to the requirements for security systems and equipment maintenance in §§ 105.250 and 106.255 to allow facility and OCS facility owners or operators to develop and follow other procedures which the owner or operator has found to be more appropriate through experience or other means.

The intent of the security systems and equipment maintenance requirement is to require the use of the manufacturer's approved procedures for maintenance. If owners or operators have found other methods to be more appropriate, they may apply for equivalents following the procedures in §§ 105.135 or 106.130.

One commenter suggested that the Coast Guard establish additional criteria for certain expensive security equipment (such as 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 or facilities.

One commenter stated that § 105.255(a) regarding access control should explicitly state that the implementation of security measures should be based on the type of cargo handled and the Facility Security Assessment.

We are not amending § 105.255(a) because, through the development of the Facility Security Assessment and Facility Security Plan, the cargo handled should be a primary consideration of a facility's vulnerability to a transportation security incident. The security measures implemented will be based on the Facility Security Assessment and Facility Security Plan, which expressly account for the facility's specific operations.

We received nine comments dealing with facility access control as it pertains to identification checks. Seven commenters asked us to add regulatory language to stipulate what will be accepted forms of identification for representatives from Federal agencies, because there is no standardized requirement for these representatives to carry their agency identification at all times and some agencies believe an officer in uniform and carrying a badge should be sufficient identification to gain access to a facility. One commenter suggested that security plans include access control measures specifically aimed at fumigators.

As part of the requirements for access control in § 105.255(e)(3), a facility owner or operator must conduct a check of the identification of any person seeking to enter the facility, including vessel passengers and crew, facility employees, Federal agency representatives, vendors (such as fumigators), personnel duly authorized by the cognizant authority, and visitors. We have provided minimum standards for identification in § 101.515, which must be met by all persons requesting access. This includes Federal agency representatives, and means that just a uniform will not be sufficient to meet the minimum standard set in § 101.515, and only those badges meeting that standard will be acceptable.

It should be noted that, with respect to Federal agency representatives, we have amended § 101.515 by adding a new provision to clarify that the identification and access control requirements of this subchapter must not be used to delay or obstruct authorized law enforcement officials from being granted access to the vessel, facility, or OCS facility. Authorized law enforcement officials are those individuals who have the legal authority to go on the vessel, facility, or OCS facility for purposes of enforcing or assisting in enforcing any applicable laws. This authority is evident by the presentation of identification and credentials that meet the requirements of § 101.515, as well as other factors such as the uniforms and markings on law enforcement vehicles and vessels. Delaying or obstructing access to authorized law enforcement officials by requiring independent verification or validation of their identification, credential, or purposes for gaining access could undermine compliance and inspection efforts, be contrary to enhancing security in some instances, and be contrary to law. Failure or refusal to permit an authorized law enforcement official presenting proper identification to enter or board a vessel, facility, or OCS facility will subject the operator or owner of the vessel, facility, or OCS facility to the penalties provided in law. In addition, an owner or operator of a vessel (including the Master), facility, or OCS facility that reasonably suspects individuals of using false law enforcement identification or impersonating a law enforcement official to gain unauthorized access, should report such concerns immediately to the COTP.

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.

Four commenters asked for amendments to §§ 105.255(c)(2) and 106.260(c)(2) to include coordination with aircraft identification systems, when practicable, in addition to coordination with vessel identification systems as a required access control measure.

We agree with the commenters, and have amended §§ 105.255(c)(2) and 106.260(c)(2) to reflect this clarification. Most facilities, including OCS facilities, are accessible by multiple forms of transportation; therefore, coordination with identification systems used by those forms of transportation should enhance security.

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 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) aboard unmanned barges to describe security measures in place is unnecessary because existing signs indicate that visitors are not permitted aboard. 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.

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, and we have required the owner or operator to ensure this is done.

We received comments from other Federal agencies requesting that government-owned vehicles on official business be exempt from screening or inspection. We have amended section 105.255(e)(1) and (f)(7) accordingly. This does not exempt government personnel from presenting identification credentials, on demand, for entry onto vessels or facilities.

One commenter requested that owners or operators of small private facilities be exempt from the requirement to screen baggage, under § 105.255, because they do not deal with passengers.

Section 105.255(e)(1) states that owners or operators must screen baggage at the rate specified in the facility's approved security plan. Because Facility Security Plans are tailored to the specific facility, it is possible that an approved plan could have very different baggage-screening provisions from a larger facility that serves multiple vessels. It is also possible that an approved plan could have provisions for coordinating baggage screening with vessels. However, we consider baggage screening an imperative security provision and have not exempted it in this final rule.

Eight commenters suggested that access control aboard OCS facilities only be required when an unscheduled vessel is forced to discharge passengers for emergency reasons, and that the provisions of § 105.255 and § 106.260 be the responsibility of the shoreside facility and the vessel owner. The commenter stated that the need to duplicate the process at the facility is wasteful. The commenters asked for amendments to § 105.255 and § 106.260 in order to make clear that security controls should be established shoreside.

The Coast Guard believes that access control must be established to ensure that the people on board any vessel or facility are identified and permitted to be there. We recognize that access control and personal identification checks at both the shoreside and OCS facility could be duplicative, and did not intend to require this duplication, unless needed. Our regulations provide the flexibility to integrate shoreside screening into OCS facility security measures. We note, however, that the OCS facility owner or operator retains ultimate responsibility for ensuring that access control measures are implemented. This means that, where integrated shoreside screening is implemented, the OCS facility owner or operator should have a means to verify that the shoreside screening is being done in accordance with the Facility Security Plan and these regulations. Even if integrated shoreside screening is arranged, the Facility Security Plan must also contain access control provisions for vessels or other types of transportation conveyances that do not regularly call on the OCS facility or might not use the designated shoreside screening process.

One commenter asked for clarification on whether fencing was required and the dates by which the construction of the fences should be accomplished, stating that fences could make normal business operations difficult.

The Coast Guard does not mandate fencing to prevent unauthorized access. Section 105.255 gives facility owners and operators the flexibility to implement those security measures that meet the specific performance standards for access control. Facilities must submit their security plan for approval by the Coast Guard on or before December 31, 2003, and must be operating under a plan approved by the Coast Guard by July 1, 2004. If a facility owner or operator intends to make physical improvements, such as installing fencing, but has not done so, this can be addressed in the Facility Security Plan. However, until improvements have been made, equivalent security measures must be explained in the Facility Security Plan and implemented.

In reviewing sections dealing with access control requirements, we noted an omission in text and 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 asked us to provide alternatives, including the use of locks, to the restricted-access control measures specified in § 105.260(d).

The measures specified in § 105.260(d) do not constitute an exclusive list; however, in § 105.260(d)(2) we specifically provide for the use of measures to secure access points that are not in active use, and this could include the use of locks.

One commenter stated that his facility could not implement the requirements of § 105.260(e)(4) regarding restricting parking adjacent to vessels because the facility does not own the area where those vehicles are parked. The commenter also stated that the facility does not own the area where vessels are unloaded.

Designating the area of the facility that is adjacent to a vessel a restricted area is of importance because vehicles may be used to cause a transportation security incident. Section 105.260(b)(1) requires, as appropriate, that areas adjacent to a vessel be designated as a restricted area. Section 105.260(e)(4) further emphasizes the importance of limiting parking near a vessel during heightened threat. The specific security measures implemented at the facility will be based on the Facility Security Assessment and Facility Security Plan, which expressly account for the facility's specific operations and the vessels it receives. Under certain circumstances, as documented in the facility security assessment report, it may be appropriate to park a properly screened vehicle alongside a vessel. However, in other circumstances it may be inappropriate based on the type of cargo and vessel involved and the current MARSEC Level. One way for a facility operator to restrict parking near the vessel is to coordinate arrangements with the neighboring facility owner so the area can be controlled. The Coast Guard will take into account issues concerning the individual responsibilities and jurisdiction of operators and the owners when reviewing the Facility Security Plan.

Two commenters suggested that § 105.265, ''Security Measures for Handling Cargo'' should state that it is applicable only to facilities that receive vessels that handle cargo.

We agree that only facilities that receive vessels that handle cargo should comply with § 105.265. Facilities that receive vessels that do not handle cargo do not have to comply with § 105.265.

One commenter stated that the language in § 105.265(c) does not define the term ''active.'' The commenter wanted to know if the Coast Guard has developed an internal interpretation as to what is meant by ''active'' access points and whether it is appropriate to assume that the facility has the discretion of identifying those access points.

Access points to the facility that can be used for entering or exiting a facility should be blocked during heightened security levels. Any access point to a facility that can be used for entering or exiting a facility is considered an active access point.

Three commenters asked for editorial revisions in § 105.265(a). One commenter asked us to revise § 105.265(a)(2), which requires facilities to ''prevent cargo that is not meant for carriage from being accepted and stored.'' The commenter stated that the section, as written, would preclude facilities from engaging in some legitimate activities such as warehousing or temporary storage. One commenter suggested adding the word ''unidentified'' before the word ''cargo'' in § 105.265(a)(6) because some facilities only store goods and do not transport them. One commenter asked why the term ''location'' is used twice in § 105.265(a)(9).

We agree with the commenter that many waterfront facilities may be used for warehousing or temporary storage of goods, etc., that are not intended for carriage in maritime commerce. We have amended § 105.265(a)(2) to make it clear that facility owners or operators can store items that will not be shipped in maritime commerce if they do so knowingly. We have not added the word ''unidentified'' in this amendment because only identified items can be stored. We have reviewed and agree that the use of the word ''location'' twice in § 105.265(a)(9) is redundant. We have amended this section to remove the redundancy.

One commenter asked us to confirm its inference that § 105.265(a)(6) allows for the legitimate accumulation of cargo for a yet to be determined vessel, or for operational reasons by either the vessel or facility operator.

We agree with the commenter's interpretation. Facility owners or operators may accept cargo that does not have a confirmed date for loading, if they determine that it is appropriate to do so under the circumstances.

Three commenters requested clarification on the restrictions of cargo entering a facility. Two commenters asked us to clarify the requirements in § 105.265(a)(6) so that its restriction on entry of cargo to a facility would only apply to break-bulk and packaged cargo shipments, and would exclude bulk-liquid facilities. One commenter asked us to exempt bulk cargo facilities from the requirements of § 105.265.

We disagree with the commenters. The intent of this regulation is to ensure that only those cargoes that have a legitimate reason for being at the facility are allowed entry. By excluding certain cargoes, as suggested by the commenters, the intent of the regulation would be weakened, and we do not see an improvement in security derived from the suggestion.

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 after they arrive 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 and 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. Screening of vehicles remains a requirement under these regulations; however, checking cargo containers may be limited to external examinations to detect signs of tampering, including checking of the integrity of seals. 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 § 104.275(b) and (c) vessel security measures for handling cargo. 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.

One commenter requested changes in the MARSEC Level 2 cargo handling provisions of § 105.265(c). The commenter stated that the container segregation provisions of paragraph (c)(5) are impractical, and that the provision in paragraph (c)(7) for limiting the number of locations where dangerous goods or hazardous substances are stored would merely create easier targets for terrorists.

We agree that the requirement in § 105.265(c)(5) could be impractical for the majority of cargo operations; however, it should be noted that this section lists various methods to use in order to meet MARSEC Level 2. It was neither an exhaustive list nor a mandated one. To list an alternative cargo handling option, we have changed § 105.265(c)(5) by removing the requirement for cargo segregation and replacing it with the option to coordinate cargo shipments with regular shippers as was mentioned in § 105.265(a). This change now aligns the facility cargo handling security measures with those found in § 104.275 for vessels, as appropriate. We did not amend § 105.265(c)(7) because we believe there may be circumstances when the requirement is desirable because it facilitates other security measures such as monitoring and access control.

Two commenters stated that fleeting facilities should not be exempt from the requirements for security measures for delivery of vessel stores and bunkers because at some fleeting areas, stores are put on board vessels, surveyors collect samples, and equipment repairs are completed.

We believe that certain activities, such as provisions being put on board vessels, surveyors collecting samples, and equipment repairs done at the fleeting facility, occur so infrequently that they would be adequately covered by the security measures of the involved vessels or barges. Those fleeting facilities where these activities routinely occur should take those activities into consideration in their Facility Security Assessments.

One commenter stated that, as detailed in § 105.270, the facility's responsibilities for the security of vessel stores are excessive. The commenter said that anything beyond validating the vendor's identity and the stores order should be the government's responsibility.

We disagree with the commenter. A facility is a vital link in the transfer of vessel stores from vendor to vessel. Our requirements focus on the safety and integrity of stores brought into the facility and on preserving stores from tampering while they are at the facility, and therefore help protect both the facility and those whom it serves.

Two commenters stated that the facility's responsibilities for the security of vessel stores as detailed in § 105.270 are less restrictive than security measures for handling cargo. The commenter recommended combining the security requirements for stores and bunkers with those requirements for handling cargo. One commenter stated that the delivery of vessel stores and bunkers are usually coordinated with the ship's agent and not the facility, and therefore the facility owner or operator should not be required to ensure that security measures are implemented.

We disagree with the commenters. We allow for the owner or operator to enact scalable measures that can provide for different levels of security. The owner or operator may enact more stringent measures for stores and bunkers to match those for handling cargo if desired. However, procedures for vessel stores and bunkers are appreciably different than procedures for most other cargo handling and usually involve different personnel; therefore, we have retained the language in § 105.270. Further, we believe that the facility owner or operator has the responsibility for providing appropriate security measures for all deliveries on the facility.

We received ten 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.

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 requires 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.

Two commenters supported the exemption from this part for those facilities that have designated public access areas. One commenter suggested that ferries be exempted from screening unaccompanied baggage. One commenter recommended that we explicitly exempt public access areas from MARSEC Level 2 and 3 passenger screening and identification requirements.

We do not intend to exempt unaccompanied baggage from screening since we believe that it is absolutely necessary to screen unaccompanied baggage. We have amended the regulations to clarify the requirements for passenger vessels, ferries, and public access areas in § 105.285 and to exempt public access areas from the MARSEC Level 2 and 3 passenger screening and identification requirements in § 105.110.

One commenter asked us to define the term ''CDC facility'' used in § 105.295, and recommended that the section should apply only when CDC is actually present on a facility.

A CDC facility is a ''facility'' that handles ''certain dangerous cargo (CDC).'' Both of these terms are defined in § 101.105. We disagree that § 105.295 should apply only when CDC is actually present on a facility, because the measures required by the section must be taken in advance so that they can be implemented when CDC is present. 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 change would be the subject of a future rulemaking.

Six commenters inquired whether § 105.295(b)(2) requires personnel to be present or if electronic equipment, such as cameras or monitors watched by personnel, may be used to satisfy the requirement.

Cameras or monitors watched by personnel could be used to meet the requirements of § 105.275, Security measures for monitoring, for MARSEC Level 1. However, the intent of § 105.295(b)(2), Additional requirements—Certain Dangerous Cargo (CDC) facilities, is to provide a higher level of security at MARSEC Level 2 or 3 for facilities handling CDCs. Guards and patrols provide a visible deterrent which we believe is an appropriate higher standard of security for CDC facilities because of the risk they pose if involved in a transportation security incident. To clarify, we are amending § 105.295(b)(2) by removing the words ''guard or'' to eliminate any ambiguity as to the need for a physical presence at a facility that handles CDC during MARSEC Levels 2 and 3. The intent of these regulations is to provide a higher level of security for these facilities.

Five commenters stated that the additional requirements for barges in fleeting facilities (as stated in § 105.296) should only apply to CDC barges at MARSEC Level 1.

We disagree that the additional requirements for barges in fleeting facilities should only apply to CDC barges at MARSEC Level 1. In order to protect the facilities and barges, the requirements applying to barges carrying CDC should also apply to those carrying cargoes subject to subchapters D or O at MARSEC Level 1.

Nine commenters stated that barges with CDC, subject to 46 CFR subchapters D or O, should be segregated ''as appropriate,'' or based on the results of a security assessment, because segregation of tank barges can be impractical when trying to assemble or break down a mixed tow and may only create a more attractive target for would-be terrorists.

We recognize that facility owners and operators need flexibility in storing and handling barges and have modified § 105.296 by removing the requirement to segregate barges carrying CDC or cargos subject to 46 CFR subchapters D or O. Instead, we have required barges carrying these cargoes to be kept within a restricted area. This will allow facility owners and operators to store other barges within the restricted area. The regulations do not prohibit or require that the assembly or break down of tows occur within the restricted area. The security measures that will be applied while assembling or breaking tows must be addressed in the Facility Security Plan. We have also amended, for clarity, the requirements of part 105 so that it only applies to those barges that carry cargo regulated under 46 CFR subchapters D or O in bulk by amending §§ 105.105 and 105.296.

Six commenters asked us to clarify whether § 105.296 requires one towing vessel per 100 barges that carry CDC.

As written, § 105.296 requires one towing vessel per 100 barges, which means any type of barge, irrespective of cargo. It should be noted that this requirement conforms to the existing 1-to-100 tug/barge ratio that already exists in 33 CFR part 165 during high water conditions.

Two commenters stated that most barge fleeting facilities are difficult to

access by land and patrolling the shoreside is impractical. One commenter stated that it would be very difficult to coordinate shore-side patrols when the facility owner does not own the land.

We recognize that it may be difficult to monitor or patrol remote barge fleeting facilities. However, we have determined that barge fleeting facilities may be involved in a transportation security incident if fleeting barges carry dangerous goods or hazardous substances. Section 105.296 does allow facility owners and operators to use monitoring in remote locations as an alternative to shore-side patrols.

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, the details of 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—Facility Security Assessment (FSA)

This subpart describes the content and procedures for Facility 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 the 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.

We received four comments regarding the use of third party companies to conduct security assessments. Two commenters asked if we will provide a list of acceptable assessment companies because of the concern that the vulnerability assessment could ''fall into the wrong hands.'' One commenter requested that the regulations define ''appropriate skills'' that a third party must have in order to aid in the development of security assessments. One commenter stated that the person or company conducting the assessment might not be reliable.

We will not be providing a list of acceptable assessment companies, nor will we define ''appropriate skills.'' It is the responsibility of the vessel or facility owner or operator to vet companies that assist them in their security assessments. In the temporary interim rule (68 FR 39254), we stated, ''we reference ISPS Code, part B, paragraph 4.5, as a list of competencies all owners and operators should use to guide their decision on hiring a company to assist with meeting the regulations. We may provide further guidance on competencies for maritime security organizations, as necessary, but do not intend to list organizations, provide standards within the regulations, or certify organizations.'' We require security assessments to be protected from unauthorized disclosures and will enforce this requirement, including through the penalties provision, in § 101.415.

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

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

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

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

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

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

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

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

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

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

nationwide consistency to strengthen maritime security without putting any particular State or region at a competitive economic disadvantage. We believe, however, that local security considerations are imperative in security plans. Our regulations do not mandate specific security measures; rather, they require the development and implementation of security assessments and plans. It is possible that security measures taken to date to fulfill State or local requirements will be sufficient to meet the new Federal requirements. These security measures may be accounted for in security assessments and should be fully documented in the security plans submitted to the Coast Guard. Local COTPs, who will review Facility Security Assessment reports and Facility Security Plans submitted under part 105, will be able to assess compliance and alignment with local, State, and Federal 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.

One commenter stated that if a Facility Security Assessment determines a threat that is outside the scope of what is appropriate to include in the Facility Security Plan, the threat should be included as part of the AMS Plan.

We agree with the commenter. The AMS Plan is more general in nature and takes into account those threats that may affect the entire port, or a segment of the port. As such, the AMS Plan should be designed to take into account those threats that are larger in scope than those threats that should be considered for individual facilities. To focus the Facility Security Assessments on their port interface rather than the broader requirement, we have amended §§ 105.305 (c)(2)(viii), (ix) and 106.305 (c)(2)(v) to reflect that the assessment of the facility should take into consideration the use of the facility as a transfer point for a weapon of mass destruction and the impact of a vessel blocking the entrance to or area surrounding a facility. Two commenters addressed the requirements of analyzing a facility's threats under § 105.305(c)(2) and (c)(3). One commenter said that the analysis of threats required by § 105.305(c)(2) and (c)(3) should be addressed in the AMS Plan and not in the Facility Security Plan because threat assessment is a government responsibility. One commenter stated that the analysis of threat information should not be required in the Facility Security Assessment because the government is best situated to assess threats.

We agree that threat analysis is part of the AMS Plan. However, a facility's security also depends in large part on how well the owner or operator assesses vulnerabilities that only he or she would know about and the consequences that could occur from the unique operations or location of the facility, as well as on the assessment of threats identified by the government. The facility's own assessment is imperative to the development of the Facility Security Plan that must identify these unique aspects and address them in a manner appropriate for the facility. Threat information, which will be issued by the Coast Guard or other agencies having knowledge of this type of information, should be considered in the Facility Security Assessment. In general, however, lacking specific threat assessment information, the facility owner or operator must assume that threats will increase against the vulnerable part of the facility and develop progressively increasing security measures, as appropriate.

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.

Three commenters noted that vulnerability assessments should take into account the type of cargo handled or transported, especially if the cargo is CDC. One commenter stated that CDCs should be carefully considered. One commenter stated that the Coast Guard should also take into account the type of cargo handled during our review of a Facility Security Assessment and Plan. One commenter noted that there is a lower risk associated with Great Lakes facilities that primarily handle dry-bulk cargoes.

We agree that security assessments and security plans should take into account the type of cargo that is handled to maximize the focus of security efforts. During our review of all assessments and plans, the Coast Guard will take into consideration types of cargo handled or transported.

After further review of subpart C of parts 104, 105, and 106, we noted the omission of detailing when the security assessment must be reviewed. Therefore, we are amending §§ 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.

Two commenters asked for clarification regarding the reference to § 105.415, ''Amendment and audit,'' found in § 105.310(a).

We reviewed § 105.310(a) and have corrected the reference to read ''§ 105.410.'' We meant for the Facility Security Assessment report to be included with the Facility Security Plan when that plan is submitted to the Coast Guard for approval under § 105.410. We are also amending §§ 105.415 and 106.310 to make similar corrections to references.

Subpart D—Facility Security Plan (FSP)

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

We received five comments asking which entity, the owner or operator, assumes responsibility for compliance and facility security. Two commenters noted that multiple companies may temporarily lease a ''dock facility,'' and questioned if each is required to submit a Facility Security Plan along with the ''dock owner.'' One commenter stated that the landlord of a facility should develop and implement a security plan and the tenants at the facility should be included in the landlord's plan. One commenter believed that 33 CFR part

105 should be clarified to state that the facility owner is the entity responsible for implementing and ensuring compliance with the facility security requirements and facility operators should be requested to address activities that are otherwise under their control, and noted that the facility operator lacked the jurisdiction to implement security measures for the entire facility.

The regulations require the owner or operator of a facility to submit a Facility Security Plan. If the facility is comprised of independent operators, then each operator is required to submit a Facility 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 operators. The Coast Guard will take into account issues concerning the individual responsibilities and jurisdiction of operators and owners when reviewing the security plan.

One commenter requested that the ''Facility Vulnerability and Security Measures Summary'' (form CG–6025) be available in electronic format and that electronic submission be available.

We agree, and have placed the form on our Port Security Directorate Web site: *http://www.uscg.mil/hq/g-m/mp/index.htm.* We are not, at this time, able to accept these forms electronically because we do not have a site capable of receiving sensitive security information. We are working on this issue, however, and hope to have this capability in the future.

We received three comments regarding access by individuals to and from vessels moored at a facility. Two commenters recommended the language in § 105.405(a)(6) be modified by adding: ''including procedures for personnel access through the facility to and from the ship'' to the end of the existing verbiage. One commenter recommended that facility owners or operators should limit access to vessels moored at the facility to those individuals and organizations that conduct business with the vessel, contending that the word ''visitors'' may be too broad.

The intent of the wording in § 105.405(a)(10) was to encompass the concept of ''including procedures for personnel access through the facility to and from the ship.'' However, the regulations provide flexibility to allow the facility to limit access to those visitors that have official business with the vessel.

Three commenters recommended that this rule 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's 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 the various dates before July 1, 2004, and after this date.

One commenter stated that § 105.410 regarding the Facility Security Plan approval process does not address what would occur if the COTP fails to approve or disapprove a plan in a timely manner and recommended that the rule include language stating that a timely submitted plan that is not approved by the COTP within 24 months be deemed to have interim approval.

As stated in § 105.120(b), if the plan has not been reviewed prior to July 1, 2004, the facility owner or operator will receive an acknowledgement letter from the COTP stating that the COTP has received the Facility Security Plan for review and approval. The facility may continue to operate so long as it remains in compliance with the submitted Facility Security Plan. We do not agree with the commenter that after 24 months, the facility should have interim approval by default.

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.

One commenter recommended that the COTP not be required to approve Facility Security Plans; rather, the COTP should ''spot-check'' facilities to see if they adhere to their plans' procedures.

We disagree. The ISPS Code requires contracting governments to approve facility security plans for facilities within their jurisdiction. Approval of a Facility Security Plan by the COTP ensures that the facility's plan aligns with the requirements of the ISPS Code, the MTSA, and these final rules. Compliance by the facility with the terms of its approved plan will be the subject of periodic Coast Guard inspection.

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.

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 insignificant failures in the Facility Security Plan discovered during exercises should not result in the need to resubmit a Facility Security Plan.

We believe that any failure of the Facility Security Plan during an exercise is a significant failure and, therefore, should be corrected. Section 105.415 provides that the COTP may determine that an amendment to a Facility Security Plan is required to maintain the facility's security.

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.

One commenter believed that § 105.415 does not provide enough flexibility in performing the annual audits of Facility Security Plans.

We disagree that the requirements of § 105.415 are not flexible enough with respect to auditing, insofar as it provides an exception to the requirements when they are ''impractical due to the size and nature of the company or the facility personnel.''

Additional Changes

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: §§ 105.105(c)(1), 105.106(a), 105.205(c)(3), 105.275(a)(1), and 105.400(b). 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 Department of Homeland Security. A ''Cost Assessment and Final Regulatory Flexibility Analysis'' 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.

Two commenters addressed the burdens involved in moving from MARSEC Level 1 to MARSEC Level 2. One strongly urged the Coast Guard to be cautious whenever contemplating raising the MARSEC Level because the commenter claimed that we estimated the cost to the maritime industry of increasing the MARSEC Level from 1 to 2 will be $31 million per day. The other commenter expressed doubt that a facility's security would be substantially increased by hiring local security personnel ''as required'' at MARSEC Level 2.

We agree that each MARSEC Level elevation may have serious economic impacts on the maritime industry. We make MARSEC Level changes in conjunction with Department of Homeland Security to ensure that the maritime sector has deterrent measures in place commensurate with the nature of the threat to it and our nation. The financial burden to the maritime sector is one of many factors that we consider when balancing security measure requirements with economic impacts. Furthermore, we disagree with the first commenter's statement of our cost assessment to the maritime industry for an increase in MARSEC Level 1 to MARSEC Level 2. In the Cost Assessment and Initial Regulatory Flexibility Act analyses for the temporary interim rules, we estimated that the daily cost of elevating the MARSEC Level from 1 to 2 is $16 million. We also disagree with the second commenter's inference that hiring local security personnel to guard a facility is required at MARSEC Level 2. Section 105.255 lists ''assigning additional personnel to guard access points'' as one of the enhanced security measures that a facility may take at MARSEC Level 2, but this can be done by reassigning the facility's own staff rather than by hiring local security personnel. Moreover it is only one of several MARSEC Level 2 security enhancements listed in § 105.255(f), which is not an exclusive list.

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.

One commenter stated that the Coast Guard should consider the impact of security regulations on facilities that face international competition.

The Coast Guard has determined that these regulations will impose significant costs on regulated facilities, and has considered the consequences of that cost. We assessed the financial impact to small businesses in the Initial and Final Cost Assessments and Regulatory Flexibility Analyses, which are found in the dockets for these rules. We were unable to specifically determine, however, which facilities face international competition.

Three commenters stated that the cost-benefit assessment in the temporary interim rule (68 FR 39276) (part 101) is questionable. One commenter noted that we did not use the most recent industry data. Two commenters stated that cost estimates might be close to accurate but that the benefits were based on assumptions that are difficult to measure.

We used the most reliable economic data available to us from the U.S. Census Bureau among other government data sources. In the notice of public meeting (67 FR 78742, December 20, 2002), we presented a preliminary cost analysis and requested comments and data be submitted to assist us in drafting our estimates. We amended our cost estimates incorporating comments and input we received. While the analysis may or may not be useful to the reader, we must develop a regulatory assessment for all significant rules, as required by Executive Order 12866.

One commenter stated that Florida laws require a double-gating standard for certain shipyards, which poses an economic burden on affected facilities, and the State of Florida has yet to conduct an economic assessment of the economic burden.

The economic impact of State security requirements is beyond the scope of these rules and is best addressed to the States imposing such requirements.

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 39319) (part 105), the costs remain unchanged.

We realize that every company engaged in maritime commerce will not implement this final rule exactly as presented in the 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 will implement this final rule differently based on the type of facilities it owns or operates and whether it engages in international or domestic trade.

The population affected by this final rule is approximately 5,000 facilities, and the estimated Present Value cost to these facilities is approximately present value $5.399 billion (2003 to 2012, 7 percent discount rate). Approximately present value $2.718 billion of this total is attributed to facilities engaged in the transfer of hazardous bulk liquids (petroleum, edible oils, and liquified gases). The remaining present value $2.681 billion is attributable to facilities that receive vessels on international voyages or carry more than 150 passengers, or fleet barges carrying certain dangerous cargoes or subchapter D or O cargoes in bulk. During the initial year of compliance, the cost is attributable to purchasing and installing equipment, hiring security officers, and preparing paperwork. The initial cost is an estimated $1.125 billion (non-discounted, $498 million for the facilities with hazardous bulk liquids, $627 million for the other facilities). Following initial implementation, the annual cost is an estimated $656 million (non-discounted, $341 million for the facilities with hazardous bulk liquids, $315 million for the other facilities).

Approximately 51 percent of the initial cost is for installing or upgrading equipment, 30 percent for hiring and training Facility Security Officers, 14 percent for hiring additional security guards, and 5 percent for paperwork (Facility Security Assessments and Facility Security Plans). Following the first year, approximately 52 percent of the annual cost is for Facility Security Officers (cost and training), 24 percent for security guards, 9 percent for paperwork (updating Facility Security Assessments and Facility Security Plans), 9 percent for operations and maintenance for equipment, and approximately 6 percent for drills. The cost of facility security consists primarily of installing or upgrading equipment and designating Facility Security Officers.

Benefit Assessment

This rule is one of six final rules that implement national maritime security initiatives concerning general provisions, Area Maritime Security, vessels, facilities, Outer Continental Shelf facilities, and Automatic Identification System (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 facility security for the affected population reduces 473,659 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 rule				
	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

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

Maritime entity	Annual risk points reduced by final rule				
	Vessel security	Facility security	OCS facility security	AMS	AIS
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 have reviewed this final rule for potential economic impacts on small entities. A Final Regulatory Flexibility Analysis discussing the impact of this final rule on small entities is available in the docket where indicated under **ADDRESSES.**

Our assessment (copy available in the docket) concludes that implementing this final rule may have a significant economic impact on a substantial number of small entities.

There are approximately 1,200 companies that own facilities that will be affected by the final rule. We researched these companies, and found revenue and business size data for 581 of them (48 percent). Of the 581, we determined that 296 are small entities according to Small Business Administration standards.

The cost of the final rule to each facility is dependent on the security measures already in place at each facility and on the relevant risk to a maritime transportation security incident. The final rule calls for specific security measures to be in place at each affected facility. We realize, however, that most facilities already have implemented security measures that may satisfy the requirements of this rule. For example, we note that every facility will develop a Facility Security Assessment and a Facility Security Plan, but not all of them may need to install or upgrade fences or lighting equipment.

For this reason, we analyzed the small entities under two scenarios, a higher cost and lower cost scenarios. The higher cost scenario uses an estimated initial cost of $1,942,500 and its corresponding annual cost of $742,700. The higher cost scenario assumed extensive capital improvements will be undertaken by the facilities in addition to the cost of complying with the minimum requirements (assigning Facility Security Officers, drafting Facility Security Assessments, drafting Facility Security Plans, conducting training, performing drills, and completing Declarations of Security). The lower cost scenario used an initial cost of $133,500 and annual cost of $156,800 for complying with the minimum requirements in the final rule.

In the higher cost scenario, we estimated that the annual revenues of 94 percent of the small entities may be impacted initially by more than 5 percent, while the annual revenues of 80 percent of the small entities may be impacted annually by more than 5 percent. In the lower cost scenario, we found that the annual revenues of 57 percent of the small entities may be impacted initially and annually by more than 5 percent.

Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 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 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.

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

As stated in the temporary interim rule (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 this regulation. 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.

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 U.S. (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 received comments regarding the taking of private property; these comments are discussed within the ''Discussion of Comments and Changes'' section of this preamble.

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) and (34)(c), of Commandant Instruction M16475.lD, this 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 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.

List of Subjects in 33 CFR Part 105

Facilities, Maritime security, Reporting and recordkeeping requirements, Security measures.

Dated: October 8, 2003.

Thomas H. Collins

Admiral, Coast Guard, Commandant.

■ Accordingly, the interim rule adding 33 CFR part 105 that was published at 68 FR 39315 on July 1, 2003, and amended at 68 FR 41916 on July 16, 2003, is adopted as a final rule with the following changes:

PART 105—MARITIME SECURITY: FACILITIES

■ 1. The authority citation for part 105 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70103; 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 105 to read as shown above.

■ 3. In § 105.105—

■ a. Revise paragraphs (a)(2), (a)(3), and (a)(4) to read as set out below;

■ b. Add paragraphs (a)(5) and (a)(6) to read as set out below;

■ c. Revise paragraphs (c)(1) and (c)(3)(i) to read as set out below;

■ d. Remove paragraph (c)(3)(ii);

■ e. Redesignate paragraph (c)(3)(iii) as paragraph (c)(3)(ii):

§ 105.105 Applicability.

(a) * * *

(2) Facility that receives vessels certificated to carry more than 150 passengers, except those vessels not carrying and not embarking or disembarking passengers at the facility;

(3) Facility that receives vessels subject to the International Convention for Safety of Life at Sea, 1974, chapter XI;

(4) Facility that receives foreign cargo vessels greater than 100 gross register tons;

(5) Facility that receives U.S. cargo vessels, greater than 100 gross register tons, subject to 46 CFR chapter I, subchapter I, except for those facilities that receive only commercial fishing vessels inspected under 46 CFR part 105; or

(6) Barge fleeting facility that receives barges carrying, in bulk, cargoes regulated by 46 CFR chapter I, subchapters D or O, or Certain Dangerous Cargoes.

* * * * *

(c) * * *

(1) A facility owned or operated by the U.S. that is used primarily for military purposes.

* * * * *

(3) * * *

(i) The facility is engaged solely in the support of exploration, development, or production of oil and natural gas and transports or stores quantities of hazardous materials that do not meet or exceed those specified in 49 CFR 172.800(b)(1) through (b)(6); or

* * * * *

■ 4. In § 105.106—

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

■ b. In paragraph (b), after the word ''provides'', add the word ''pedestrian''.

§ 105.106 Public access areas.

(a) A facility serving ferries or passenger vessels certificated to carry more than 150 passengers, other than cruise ships, may designate an area within the facility as a public access area.

* * * * *

■ 5. In § 105.110, revise paragraph (b) and add paragraphs (c), (d), and (e) to read as follows:

§ 105.110 Exemptions.

* * * * *

(b) A public access area designated under § 105.106 is exempt from the requirements for screening of persons, baggage, and personal effects and identification of persons in § 105.255(c), (e)(1), (e)(3), (f)(1), and (g)(1) and § 105.285(a)(1).

(c) An owner or operator of any general shipyard facility as defined in § 101.105 is exempt from the requirements of this part unless the facility:

(1) Is subject to parts 126, 127, or 154 of this chapter; or

(2) Provides any other service to vessels subject to part 104 of this subchapter not related to construction, repair, rehabilitation, refurbishment, or rebuilding.

(d) *Public access facility.* (1) The COTP may exempt a public access facility from the requirements of this part, including establishing conditions for which such an exemption is granted, to ensure that adequate security is maintained.

(2) The owner or operator of any public access facility exempted under this section must:

(i) Comply with any COTP conditions for the exemption; and

(ii) Ensure that the cognizant COTP has the appropriate information for contacting the individual with security responsibilities for the public access facility at all times.

(3) The cognizant COTP may withdraw the exemption for a public access facility at any time the owner or operator fails to comply with any requirement of the COTP as a condition of the exemption or any measure ordered by the COTP pursuant to existing COTP authority.

(e) An owner or operator of a facility is not subject to this part if the facility receives only vessels to be laid-up, dismantled, or otherwise placed out of commission provided that the vessels are not carrying and do not receive cargo or passengers at that facility.

■ 6. In § 105.115—

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

■ b. In paragraph (b), remove the date ''June 30, 2004'' and add, in its place, the date ''July 1, 2004'':

§ 105.115 Compliance dates.

(a) On or before December 31, 2003, facility owners or operators must submit to the cognizant COTP for each facility—

(1) The Facility 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 facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

* * * * *

§ 105.120 [Amended]

■ 7. In § 105.120—

■ a. In the introductory text, remove the words ''no later than'' and add, in their place, the words ''on or before''; and

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

■ 8. Revise § 105.125 to read as follows:

§ 105.125 Noncompliance.

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

■ 9. In § 105.200—

■ a. Revise paragraph (b)(7) to read as set out below;

■ b. In paragraph (b)(8), remove the word ''and'';

■ c. Revise paragraph (b)(9) to read as set out below; and

■ d. Add paragraphs (b)(10) and (b)(11) to read as follows:

§ 105.200 Owner or operator.

* * * * *

(b) * * *

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

* * * * *

(9) Ensure security for unattended vessels moored at the facility;

(10) Ensure the report of all breaches of security and transportation security incidents to the National Response Center in accordance with part 101 of this chapter; and

(11) Ensure consistency between security requirements and safety requirements.

§ 105.205 [Amended]

■ 10. In § 105.205—

■ a. In paragraph (b)(2)(iv), remove the word ''Risk'' and add, in its place, the word ''Security'';

■ b. In paragraph (c)(3), after the words ''if necessary'', remove the word ''if'' and add, in its place, the word ''that''; and

■ c. In paragraph (c)(11), remove the words ''Vessel Security Officers'' and add, in their place, the words ''Masters, Vessel Security Officers or their designated representatives''.

§ 105.215 [Amended]

■ 11. In § 105.215, in the introductory paragraph, after the words ''in the following'', add the words '', as appropriate''.

■ 12. In § 105.220, revise paragraph (a) to read as follows:

§ 105.220 Drill and exercise requirements.

(a) *General.* (1) Drills and exercises must test the proficiency of facility personnel in assigned security duties at all MARSEC Levels and the effective implementation of the Facility Security Plan (FSP). They must enable the Facility Security Officer (FSO) 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 FSP as the result of an increase in the MARSEC Level, provided the facility reports attainment to the cognizant COTP.

* * * * *

§ 105.225 [Amended]

■ 13. In § 105.225(b)(1), remove the words ''each security training session'' and add, in their place, the words ''training under § 105.210''.

■ 14. Revise § 105.245(d) to read as follows:

§ 105.245 Declaration of Security (DoS).

* * * * *

(d) At MARSEC Levels 2 and 3, the FSOs, or their designated representatives, of facilities interfacing with manned vessels subject to part 104, of this subchapter must sign and implement DoSs as required in (b)(1) and (2) of this section.

* * * * *

§ 105.255 [Amended]

■ 15. In § 105.255—

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

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

■ c. In paragraph (c)(2), after the word ''vessels'', add the words ''or other transportation conveyances'';

■ d. In paragraph (e)(1), remove the words ''including delivery vehicles'' and, after the words ''approved FSP'' add the words '', excluding government-owned vehicles on official business when government personnel present identification credentials for entry''; and

■ e. In paragraph (f)(7), remove the word ''Screening'' and add, in its place, the words ''Except for government-owned vehicles on official business when government personnel present identification credentials for entry, screening''.

■ 16. In § 105.265—

■ a. In paragraph (a)(2), after the words ''stored at the facility'', add the words ''without the knowing consent of the facility owner or operator'';

■ b. Revise paragraphs (a)(8) and (a)(9) to read as set out below;

■ c. Remove paragraph (a)(10);

■ d. In paragraph (b)(1), remove the word ''Routinely'', and add, in its place, the words ''Unless unsafe to do so, routinely'' and remove the words ''to deter'' and add, in their place, the words ''for evidence of'';

■ e. In paragraph (c)(1), remove the word ''port'' and remove the words ''dangerous substances and devices to the facility and vessel'' and add, in their place, the words ''evidence of tampering''; and

■ f. Revise paragraph (c)(5) to read as follows:

§ 105.265 Security measures for handling cargo.

(a) * * *

(8) When there are regular or repeated cargo operations with the same shipper, coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedure; and

(9) Create, update, and maintain a continuous inventory of all dangerous goods and hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods and hazardous substances.

* * * * *

(c) * * *

(5) Coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures;

* * * * *

§ 105.275 [Amended]

■ 17. In § 105.275(a) introductory text, after the word ''patrols,'', remove the word ''and''.

■ 18. In § 105.285—

■ a. In paragraph (a) introductory text, remove the words ''At MARSEC Level 1'' and add, in their place, the words ''At all MARSEC Levels'';

■ b. In paragraph (a)(1), remove the words ''In a facility with no public access area designated under § 105.106, establish'' and, add in their place, the word ''Establish'';

■ c. In paragraph (a)(5), remove the words ''and conduct screening of persons and personal effects, as needed''; and

■ d. Revise paragraphs (b) and (c) to read as follows:

§ 105.285 Additional requirements—passenger and ferry facilities.

* * * * *

(b) At MARSEC Level 2, in addition to the requirements in paragraph (a) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under § 105.106 must increase the intensity of monitoring of the public access area.

(c) At MARSEC Level 3, in addition to the requirements in paragraph (a) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under § 105.106 must increase the intensity of monitoring and assign additional security personnel to monitor the public access area.

§ 105.295 [Amended]

■ 19. In § 105.295(b)(2), remove the words ''guard or''.

■ 20. Revise § 105.296(a)(1) to read as follows:

§ 105.296 Additional requirements-barge facilities.

(a) * * *

(1) Designate one or more restricted areas within the barge fleeting facility to handle those barges carrying, in bulk, cargoes regulated by 46 CFR chapter I, subchapters D or O, or Certain Dangerous Cargoes;

* * * * *

■ 21. In § 105.305—

■ a. In paragraph (c)(2)(viii) remove the word ''Blockage'' and add, in its place, the words ''Impact on the facility and its operations due to a blockage'';

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

■ c. Add paragraphs (d)(3), (d)(4), (d)(5), and (e) to read as follows:

§ 105.305 Facility Security Assessment (FSA) requirements.

* * * * *

(c) * * *

(2) * * *

(ix) Use of the facility as a transfer point for nuclear, biological, radiological, explosive, or chemical weapons;

* * * * *

(d) * * *

(3) The FSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) Facility personnel;

(ii) Passengers, visitors, vendors, repair technicians, vessel personnel, etc.;

(iii) Capacity to maintain emergency response;

(iv) Cargo, particularly dangerous goods and hazardous substances;

(v) Delivery of vessel stores;

(vi) Any facility security communication and surveillance systems; and

(vii) Any other facility security systems, if any.

(4) The FSA report must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on facility personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The FSA report must discuss and evaluate key facility measures and operations, including:

(i) Ensuring performance of all security duties;

(ii) Controlling access to the facility, through the use of identification systems or otherwise;

(iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);

(iv) Procedures for the handling of cargo and the delivery of vessel stores;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring the facility and areas adjacent to the pier; and

(vii) The ready availability of security communications, information, and equipment.

(e) The FSA, FSA report, and FSP must be protected from unauthorized access or disclosure.

■ 22. In § 105.310—

■ a. In paragraph (a), remove the words ''§ 105.415 of this part'' and add, in its place, the text ''§ 105.410 of this part''; and

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

§ 105.310 Submission requirements.

* * * * *

(c) The FSA must be reviewed and validated, and the FSA report must be updated each time the FSP is submitted for reapproval or revisions.

§ 105.400 [Amended]

■ 23. In § 105.400(b), in the second sentence remove the word ''Format'', and add, in its place, the word ''Information''.

■ 24. In § 105.410—

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

■ b. In paragraph (c)(1), remove the text '', or'' and add, in its place, a semicolon;

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

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

§ 105.410 Submission and approval.

(a) On or before December 31, 2003, the owner or operator of each facility currently in operation must either:

(1) Submit one copy of their Facility Security Plan (FSP) for review and approval to the cognizant COTP and a letter certifying that the FSP meets applicable requirements of this part; or

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

(b) Owners or operators of facilities 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

* * * * *

■ 25. In § 105.415—

■ a. In paragraph (a)(1), remove the word ''FSP'' and add, in its place, the words ''Facility Security Plan (FSP)'';

■ b. In paragraph (a)(2), remove the words ''§ 105.415 of this subpart'' and add, in their place, the words ''§ 105.410 of this subpart'';

■ c. Redesignate paragraph (a)(3) as (a)(4);

■ d. Add new paragraph (a)(3) to read as set out below;

■ e. In newly redesignated paragraph (a)(4), remove the words ''Facility Security Plan (FSP)'' and add, in their place, the word ''FSP'', and remove the words ''§ 105.415 if this subpart'' and add, in their place, the words ''§ 105.410 of this subpart''; and

■ f. In paragraph (b)(5), remove the words ''§ 105.415 of this subpart'' and add, in their place, the word ''§ 105.410 of this subpart'';

§ 105.415 Amendment and audit.

(a) * * *

(3) Nothing in this section should be construed as limiting the facility owner or operator from the timely implementation of such additional security measures not enumerated in the approved FSP as necessary to address exigent security situations. In such cases, the owner or operator must notify the cognizant COTP 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.

* * * * *

■ 26. In Appendix A to Part 105, revise the first page to Form CG–6025 to read as follows:

BILLING CODE 4910–15–U

Appendix A to Part 105—Facility Vulnerability and Security Measures Summary (Form CG–6025)

U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-6025 (05/03)	**FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY**	OMB APPROVAL NO. 1625-0077

An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 60 minutes. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: Commandant (G-MP), U.S. Coast Guard, 2100 2nd St, SW, Washington D.C. 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0077), Washington, DC 20503.

FACILITY IDENTIFICATION

1. Name of Facility

2. Address of Facility

3. Latitude

4. Longitude

5. Captain of the Port Zone

6. Type of Operation (check all that apply)

- ☐ Break Bulk
- ☐ Dry Bulk
- ☐ Container
- ☐ RO-RO
- ☐ Petroleum
- ☐ Chemical
- ☐ LHG/LNG
- ☐ Explosives and other dangerous cargo
- ☐ Certain Dangerous Cargo
- ☐ Barge Fleeting
- ☐ Offshore Support
- ☐ Passengers (Subchapter H)
- ☐ Passengers (Ferries)
- ☐ Passengers (Subchapter K)
- ☐ Military Supply
- ☐ If other, explain below:

VULNERABILITY AND SECURITY MEASURES

7a. Vulnerability

7b. Vulnerability Category

☐ If other, explain

8a. Selected Security Measures (MARSEC Level 1)

8b. Security Measures Category

☐ If other, explain

9a. Selected Security Measures (MARSEC Level 2)

9b. Security Measures Category

☐ If other, explain

10a. Selected Security Measures (MARSEC Level 3)

10b. Security Measures Category

☐ If other, explain

VULNERABILITY AND SECURITY MEASURES

7a. Vulnerability

7b. Vulnerability Category

☐ If other, explain

8a. Selected Security Measures (MARSEC Level 1)

8b. Security Measures Category

☐ If other, explain

9a. Selected Security Measures (MARSEC Level 2)

9b. Security Measures Category

☐ If other, explain

10a. Selected Security Measures (MARSEC Level 3)

10b. Security Measures Category

☐ If other, explain

[FR Doc. 03–26348 Filed 10–20–03; 8:45 am]

BILLING CODE 4910–15–C