



Federal Register

Wednesday,
October 22, 2003

Part II

Department of Homeland Security

Coast Guard

33 CFR Parts 2, 101, et al.

46 CFR Parts 2, 31, et al.

**National Maritime Security Initiatives;
Area Maritime Vessel, Facility, and Outer
Continental Shelf Security; Automatic
Identification System, Vessel Carriage
Requirement; Final Rules**

DEPARTMENT OF HOMELAND SECURITY**Coast Guard****33 CFR Parts 2, 101 and 102**

[USCG-2003-14792]

RIN 1625-AA69

Implementation of National Maritime Security Initiatives

AGENCY: Coast Guard, DHS.

ACTION: Final rule.

SUMMARY: The Coast Guard has published a series of final rules in today's **Federal Register** that adopt, with changes, the series of temporary interim rules published July 1, 2003, which promulgate maritime security requirements mandated by the Maritime Transportation Security Act of 2002.

This final rule establishes the general regulations for maritime security and provides the summary of the cost and benefit assessments for the entire suite of final rules published today. The discussions provided within each of the other final rules are limited to the specific requirements they contain.

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-2003-14792 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>.

You may inspect the material incorporated by reference at room 1409, U.S. Coast Guard Headquarters, 2100 Second Street SW., Washington, DC 20593-0001 between 8:30 a.m. and 3:30 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-267-6277. Copies of the material are available as indicated in the "Incorporation by Reference" section of this preamble.

FOR FURTHER INFORMATION CONTACT: If you have questions on this final rule, call Captain Kevin Dale (G-MPS), U.S. Coast Guard by telephone 202-267-6193 or by electronic mail at kdale@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 "Implementation of National Maritime Security Initiatives" in the **Federal Register** (68 FR 39240). This temporary interim rule was one of six temporary interim rules published in the July 1, 2003, issue of the **Federal Register**, each addressing maritime security. On July 16, 2003, we published a document correcting typographical errors and omissions in that rule (68 FR 41914).

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

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

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

In the aftermath of September 11, 2001, the Commandant of the Coast Guard reaffirmed the Coast Guard's Maritime Homeland Security mission and its lead role-in coordination with the Department of Defense; Federal, State, Indian Tribal, and local agencies; owners and operators of vessels and marine facilities; and others with interests in our nation's Marine Transportation System (MTS)—to detect, deter, disrupt, and respond to attacks against U.S. territory, population, vessels, facilities, and critical maritime infrastructure by terrorist organizations.

In November 2001, the Commandant of the Coast Guard addressed the International Maritime Organization (IMO) General Assembly, urging that body to consider an international scheme for port and shipping security. Recommendations and proposals for comprehensive security requirements, including amendments to the International Convention for Safety of Life at Sea, 1974, (SOLAS) and the new International Ship and Port Facility Security Code (ISPS Code), were developed at a series of intersessional maritime security work group meetings held at the direction of the IMO's Maritime Safety Committee.

The Coast Guard submitted comprehensive security proposals in January 2002 to the intersessional maritime security work group meetings based on work we had been coordinating since October 2001. Before each intersessional meeting, the Coast Guard held public meetings and coordinated several outreach meetings with representatives from major U.S. and foreign associations for shipping, labor, and ports. We also discussed maritime security at each of our Federal Advisory Committee meetings and held meetings with other Federal agencies with security responsibilities.

On January 28-30, 2002, the Coast Guard held a public workshop in Washington, DC, attended by more than 300 individuals, including members of the public and private sectors, and representatives of the national and international marine community (66 FR 65020, December 17, 2001; docket number USCG-2001-11138). Their comments indicated the need for specific threat identification, analysis of threats, and methods for developing performance standards to plan for response to maritime threats. Additionally, the public comments stressed the importance of uniformity in the application and enforcement of requirements and the need to establish

threat levels with a means to communicate threats to the MTS.

At the Marine Safety Committee's 76th session and subsequent discussions internationally, we considered and advanced U.S. proposals for maritime security that took into account this public and agency input. The Coast Guard considers both the SOLAS amendments and the ISPS Code, as adopted by the IMO Diplomatic Conference in December 2002, to reflect current industry, public, and agency concerns. The entry into force date of both the ISPS Code and related SOLAS amendments is July 1, 2004, with the exception of the Automatic Identification System (AIS). The AIS implementation date for vessels on international voyages was accelerated to no later than December 31, 2004, depending on the particular class of SOLAS vessel.

Domestically, the Coast Guard had existing regulations for the security of large passenger vessels, found in 33 CFR parts 120 and 128. The Coast Guard issued complementary guidance in the Navigation and Vessel Inspection Circular (NVIC) 3-96, Change 1, Security for Passenger Vessels and Passenger Terminals. Prior to development of additional regulations, the Coast Guard, with input from the public, assessed the current state of port and vessel security and their vulnerabilities. To accomplish this, the Coast Guard conducted the previously mentioned January 2002 public workshop to assess existing MTS security standards and measures and to gather ideas on possible improvements. Based on the comments received at the workshop, the Coast Guard cancelled NVIC 3-96 (Security for Passenger Vessels and Passenger Terminals) and issued a new NVIC 4-02 (Security for Passenger Vessels and Passenger Terminals), which was developed in conjunction with the International Council of Cruise Lines, that incorporated guidelines consistent with international initiatives (the ISPS Code and SOLAS). Additional NVICs were also published to further guide maritime security efforts, including NVIC 9-02 (Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports), NVIC 10-02 (Security Guidelines for Vessels), and NVIC 11-02 (Security Guidelines for Facilities). The documents are available in the public docket (USCG-2002-14069) for review at the locations under **ADDRESSES**.

Organization

We have kept the maritime security regulations segmented in six separate

final rules. For ease of reading and comprehension, the final rules carry the same organization as the temporary interim rules. Five of the final rules complete the new subchapter H, which was added by the temporary interim rules, in chapter I of title 33 of the Code of Federal Regulations (subchapter H). The final rule "Automatic Identification System; Vessel Carriage Requirement" (USCG-2003-14757), published elsewhere in today's **Federal Register**, finalizes the changes made to parts 26, 161, 164, and 165 in Title 33 of the Code of Federal Regulations regarding AIS. A brief description of each of the six final rules follows:

1. *Implementation of National Maritime Security Initiatives*. In the preamble to this final rule (USCG-2003-14792), we discuss the background and purpose for all of the final rules. We discuss the comments and changes made to parts 101 and 102 of the new subchapter H. We also include a summary of the costs and benefits associated with implementing the requirements of subchapter H, as well as the AIS final rule.

2. *Area Maritime Security (AMS)*. In the preamble of the "Area Maritime Security" final rule (USCG-2003-14733), found elsewhere in today's **Federal Register**, we discuss the comments and changes made to part 103 of subchapter H and discuss the cost and benefit assessment specific to that part.

3. *Vessel Security*. In the preamble of the "Vessel Security" final rule (USCG-2003-14749), found elsewhere in today's **Federal Register**, we discuss the comments and changes made to part 104 of subchapter H, to 33 CFR part 160, and to 46 CFR parts 2, 31, 71, 91, 115, 126, and 176. We also discuss the cost and benefit assessments specific to those parts.

4. *Facility Security*. In the preamble of the "Facility Security" final rule (USCG-2003-14732), found elsewhere in today's **Federal Register**, we discuss the comments and changes made to part 105 of subchapter H and discuss the cost and benefit assessments specific to that part.

5. *Outer Continental Shelf (OCS) Facility Security*. In the preamble of the "Outer Continental Shelf Facility Security" final rule (USCG-2003-14759), found elsewhere in today's **Federal Register**, we discuss the comments and changes to part 106 of subchapter H and discuss the cost and benefit assessments specific to that part.

6. *Automatic Identification Systems (AIS)*. In the preamble of the "Automatic Identification System; Vessel Carriage Requirement" final rule

(USCG-2003-14757), found elsewhere in today's **Federal Register**, we discuss the comments and changes made to 33 CFR parts 26, 161, 164, and 165 and discuss the cost and benefit assessments specific to those parts.

Coordination With SOLAS Requirements

For each of the final rules, the requirements of the Maritime Transportation Security Act (MTSA), section 102, align, where appropriate, with the security requirements in the SOLAS amendments and the ISPS Code. However, the MTSA has a broader application that includes domestic vessels and facilities. Thus, where appropriate, we have implemented the MTSA through the requirements in the SOLAS amendments and the ISPS Code, parts A and B. Further discussion on this coordination can be found in the preamble of the temporary interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792), under "Coordination with SOLAS Requirements."

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 concerns definitions, applicability, equivalents, and other subjects of a general nature applicable to all of subchapter H.

Two commenters requested that the authority citation for 46 CFR part 107 include the following citations: 46 U.S.C. Chapter 701; Executive Order 12234; 45 FR 58801; 3 CFR, 1980 Comp., p. 277; Executive Order 12777, 56 FR 54757, 3 CFR, 1991 Comp., p. 351; and Department of Homeland Security Delegation No. 0170.1.

We are not amending the authority citation because the regulations in 46 CFR part 107 are not issued under the citations that the commenters propose to add. Additionally, these changes are beyond the scope of this final rule.

We received five comments regarding our implementation of the regulations. Three commenters strongly supported the implementation of the rules, stating that maritime entities should be regulated by a single law. One commenter supported the Coast Guard's implementation of the regulations as written, because of a security breach that occurred on a ferry within the past year. One commenter acknowledged and commended the Coast Guard for the positive way it responded to previously submitted comments.

Two commenters commended the Coast Guard for ensuring that the interim rules resembled, in large part, the requirements adopted in the SOLAS amendments and the ISPS Code.

We received 10 comments on the Coast Guard's interaction with other Federal agencies. Seven commenters pointed out the need for consistency and integration throughout the Department of Homeland Security (DHS) and other Federal agencies in matters affecting maritime security. Another commenter asked us to work with the Nuclear Regulatory Commission to develop consistent and compatible regulations. One commenter stated that the Coast Guard should develop a memorandum of understanding with the Bureau of Customs and Border Protection (BCBP) to clarify the roles of the two agencies.

We agree with the commenters regarding the need for consistency and integration throughout DHS and other Federal agencies. In developing our regulations, we worked closely with many other agencies of DHS (*e.g.*, the Transportation Security Administration (TSA), BCBP), the Department of Transportation (DOT) (*e.g.*, the Maritime Administration (MARAD), the Research and Special Programs Administration (RSPA)), the Environmental Protection Agency (EPA), the Department of Energy (DOE), and the Minerals Management Service (MMS), among others. These regulations reflect input from all the Federal agencies that have a responsibility in the development and implementation of homeland security regulations covering all modes of transportation. We intend to continue these close working relationships as additional issues come to light, and we will continue to define each of our roles to ensure coordination and avoid duplication. Coordination with State and local agencies will be addressed in

the plan developed by each AMS Committee, which is established by the cognizant COTP.

We received comments from EPA regarding the effects of our regulations on EPA-regulated oil facilities. These comments focused primarily on the potential overlapping provisions of 33 CFR part 105 and 40 CFR part 112. Overlap exists in four major areas: Notification of security incidents, fencing and monitoring, evacuation procedures, and security assessments. In cases of overlapping provisions for oil facilities regulated both in parts 105 and 112, the requirements in our final rules and EPA rulemakings do not supplant one another. Additionally, an EPA-regulated facility need not amend the facility's Spill Prevention Control and Countermeasure Plan or Facility Response Plan, as we first stated in the temporary interim rule (68 FR 39251) (part 101). We will be working further with EPA in the implementation of these final rules to minimize the burden to the facilities while ensuring that these facilities are secure. It is our belief that response plans for EPA-regulated oil facilities will serve as an excellent foundation for security plans that may be required under our regulations.

EPA asked for clarification for facilities adjacent to the navigable waters that handle or store cargo that is hazardous or a pollutant but may not be marine transportation related facilities. These facilities are covered by parts 101 through 103 of subchapter H 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 Maritime Security (MARSEC) Levels that may apply to them. The AMS Assessment may reveal that these EPA-regulated facilities may be involved in a transportation security incident and the COTP may direct these facilities, through orders issued under existing COTP authority, to implement security measures based on the facilities' operations and the MARSEC Level. We encourage owners and operators of these EPA-regulated facilities, as well as representatives from EPA, to participate in AMS Committee activities.

EPA asked for further clarification on drills and exercises requirements. As we stated in the temporary interim rule, non-security drills and exercises may be combined with security drills to minimize burden. Additionally, EPA-regulated facilities that conduct drills not related to security are encouraged to communicate with the local COTP and coordinate their drills at the area level. It is our intention to give facilities and vessels in the port area as much notice

as practicable prior to an AMS Plan exercise to reduce the burden to those entities. Again, we encourage owners and operators of these EPA-regulated facilities, and EPA, to participate in AMS Committee activities to maximize coordination and minimize burden.

EPA asked us to clarify the role of Area Contingency Plans with the requirements of our final rules. Our rules are intended to work in concert with Area Contingency Plans and do not preempt their requirements. We envision that many members of the Area Committees who are responsible for implementing Area Contingency Plans will also become members of the AMS Committee. This participation will help ensure that implementing an AMS Plan will not conflict with an Area Contingency Plan.

Finally, EPA asked for clarification on requirements for marine transportation related facilities that handle petroleum oil, non-petroleum oil, and edible oil. These facilities are directly regulated under § 105.105(a)(1) and must meet the requirements of part 105.

One commenter emphasized the importance of working with State homeland security representatives to resolve any State and local issues or barriers that might interfere with providing appropriate security for the maritime industry.

We stated in the temporary interim rule (68 FR 39255) (part 101) that we consider standards for private security guards a matter of private contract and of State and local law. We believe that it is important to encourage the review of these standards, and therefore intend to work with State homeland security representatives to resolve any issues or barriers with regard to these State and local standards.

Two commenters requested that we add to § 101.100 a new paragraph that would read: "maritime security plans developed under these regulations and approved by the Coast Guard prepare vessel owners and operators, vessel crews, facility owners and operators, and facility personnel to deter to the maximum extent practicable maritime security incidents. The security measures identified in the plans provide deterrence and are not performance standards. The plans are approved on a set of assumptions regarding the security vulnerabilities recognized at the time of approval that may not be valid in an actual maritime security incident." The commenters stated that this paragraph would mirror the language of OPA 90 and clarify the intent of the subchapter.

We agree, in part, with the commenters and have amended

§ 101.100. However, to remain broad and consistent with the tone of the subchapter, we have rephrased the concept. In addition, we have made an editorial correction to § 101.100(a) to clarify that the “purpose” section applies to the entire subchapter.

The following discussion on § 101.105, Definitions, is detailed alphabetically to align, as much as possible, with the order of the terms listed in the section.

Two commenters recommended deleting the language in the definition of § 101.105 that explains that an AMS Committee can be a Port Security Committee established pursuant to NVIC 09–02, noting that this additional language is adequately covered by the regulations in part 103.

We agree that the additional language in the definition of AMS Committee is adequately explained in part 103, but we prefer to include this language for absolute clarity.

After reviewing the applicability of this subchapter to barge fleeting facilities, we determined that our reference to the Army Corps of Engineers permitting regulations in 33 CFR part 322 was not a complete representation of inland river permitting practices. Therefore, we have amended the definition of “barge fleeting facility” to clarify that these regulations apply to any barge fleeting facility permitted by the Army Corp of Engineers, whether under an individual permit, or a national or regional general permit. We believe that any barge fleeting area constitutes an obstacle under the definition of “structure” found in the Army Corps of Engineers regulations at 33 CFR 322.2.

One commenter asked us to define “breach of security” to clarify the intent of the regulations.

We agree with the commenter, and have added a definition for “breach of security” to § 101.105.

After reviewing the applicability of this subchapter to certain industrial vessels, we determined that vessels operating solely with dredge spoils may not be involved in a transportation security incident. Therefore, we amended the definition of “cargo” to clarify that dredge spoils are not considered cargo for purposes of part 104 of this chapter. This has the effect of removing certain dredges from coverage under part 104.

Eleven commenters requested that the Coast Guard clarify “Certain Dangerous Cargo” (CDC), stating that the rules should have one definition.

There is one definition for CDC that applies to all of the security regulations in subchapter H. Section 101.105

defines CDC as meaning “the same as defined in 33 CFR 160.203.” These comments revealed the need to correct the citation; the correct reference should be § 160.204, rather than § 160.203. We have amended § 101.105 accordingly. It should be noted that this change ensures consistency in Title 33. We are constantly reviewing and, when necessary, revising the CDC list based on additional threat and technological information. Changes to § 160.204 would affect the regulations in 33 CFR subchapter H because any changes to the CDC list would also affect the applicability of subchapter H. Any such changes would be the subject of a future rulemaking.

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

We agree that effective communication may be established between the Company Security Officer and one or more COTPs and that for some companies, effective communications with the Coast Guard may be at the District, Area, or Headquarters level; therefore, we are amending the definition of “Company Security Officer” in § 101.105 to remove the specific reference to the COTP.

After further review of the regulations, we are adding the definition of “dangerous goods and/or hazardous substances” to clarify the use of that term within the regulations.

Three commenters asked for clarification on dangerous substances and devices. Two commenters stated that the definition of “Dangerous substances and devices” is too broad and could be construed to include illegal drugs, plants, “and even Cuban cigars.” The commenter noted, “normal screening methods (x-ray and explosive-sniffing canines or wands) will not detect ‘substances’ nor are they necessarily an item that will cause ‘damage or injury.’” The commenter recommended amending the definition of “Dangerous substances and devices” to: (1) Specify that such substances and devices included only those that have “the potential to cause a transportation security incident”; (2) add weapons, incendiaries, and explosives; and (3) specify that such substances and devices do not include drugs, alcohol, or “other chemical or biological items not normally associated with transportation security screening.” One commenter asked how to handle legal dangerous substances, such as fertilizer and gasoline.

We agree that the definition of dangerous substances and devices could

be subject to differing interpretations. We therefore revised and simplified this definition by relating it to the potential of the dangerous substance or device to cause a transportation security incident similar to the commenter’s recommendation. However, we disagree that we need to expressly exclude the items suggested because a transportation security incident is defined as a security incident resulting in a “significant” loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. We believe the definition of a transportation security incident is such that alcoholic beverages and drugs could not be interpreted as dangerous substances and devices as the term has been redefined. Such dangerous substances and devices would include, but not be limited to, explosives, incendiaries, and assault weapons.

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

We find that the terms “vessel-to-vessel activity” and “vessel-to-vessel interface” are comparable and have chosen to use the term “vessel-to-vessel activity” to align these regulations with the ISPS Code. We have amended the definition of “Declaration of Security” in § 101.105 as well as §§ 104.105 and 104.255 to use the term “vessel-to-vessel activity” in place of “vessel-to-vessel interface,” for consistency.

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 including 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 and 105.110 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.

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

With regard to the definition of “facility” and the suggested additional language regarding MODUs, the definition clearly incorporates MODUs that are not covered under part 104 and MODUs are sufficiently covered under parts 101 through 103 and 106. Therefore, we are not amending our definition of facility nor incorporating the suggested explicit exemption from part 105 because these MODUs are excluded. We have, however, amended the applicability section of part 104 (§ 104.105) so that foreign flag, non-self propelled MODUs that meet the threshold characteristics set for OCS facilities are regulated by 33 CFR part 106, rather than 33 CFR part 104. We have done so because MODUs act and function more like OCS facilities, have limited interface activities with foreign and U.S. ports, and their personnel undergo a higher level of scrutiny to obtain visas to work on the Outer Continental Shelf. These amendments to § 104.105 required us to add a definition for “cargo vessel” in § 101.105. With these changes, we believe the existing definitions of “facility” and “OCS facility” in § 101.105 are sufficient to

conclusively identify those entities that are subject to parts 104, 105, and 106. In addition, the definition of “OCS facility,” as written, ensures that these entities will be subject to relevant elements of an OCS Area Maritime Security Plan. We believe the language in § 106.105, read in concert with the amended § 104.105(a)(1), and the existing definitions in part 101, is sufficient to preclude MODUs that are in compliance with part 104 from being subject to part 106.

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

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

Two commenters proposed language to clarify the definition of “OCS facility” to make clear that the term includes MODUs when attached to the subsoil or seabed for the exploration, development, or production of oil or natural gas. One commenter suggested that this additional language would “provide clarification regarding the applicability of” part 106.

The purpose of the broad definition of “OCS facility” in § 101.105 is to incorporate all such facilities so that the OCS facilities that are not regulated under part 106 will be regulated under

parts 101 through 103. The proposed additional language would not add clarity to part 106 because the applicability in § 106.105 states that the section applies only to those MODUs that are operating for the purposes of engaging in the exploration, development, or production of oil, natural gas, or mineral resources.

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

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

Two commenters suggested amending the definition of "owner or operator" so that the definition includes, for OCS facilities: "the lessee or the operator designated to act on behalf of the lessee in accordance with 30 CFR part 250." One commenter sought clarification of the terms "owner or operator" and suggested adding "operational control is the ability to influence or control the physical or commercial activities pertaining to that facility for any period of time."

We disagree with adding the suggested language of the first commenter because we have concluded that the owner and the person with operational control are in the best position to implement these regulations and, therefore, should be responsible for implementation. The language proposed would include a lessee regardless of whether or not that lessee maintains such operational control. We also disagree with adding the suggested language of the second comment because it does not provide for security activities in addition to the physical or commercial activities.

After further review of the definition for passenger vessel, we determined that a clarification was needed with respect to vessels on international voyages. In the temporary interim rule we unintentionally included all vessels carrying more than 12 passengers because we did not specify that a vessel on an international voyage would be deemed a passenger vessel only if it carried a passenger-for-hire. We have amended the definition to clarify that when a vessel is on an international voyage carrying more than 12 passengers, a vessel is considered a passenger vessel only if one of those passengers is a passenger-for-hire. We

have made a conforming amendment to § 104.105.

Three commenters requested that the Coast Guard clarify the term "persons" to exclude crewmembers.

We do not provide a specific definition for the term "persons" in these rules. It was our intent for the word "persons" to include crewmembers.

We received five comments regarding the use of the word "port" in the regulations. Four commenters requested that we amend many sections of parts 101 and 103 to remove the word "port" from the regulatory text, stating that parts 101 and 103 are not necessarily applicable to just ports, but to an area as a whole. One commenter recommended that we include definitions for "Seaport," "Port Authority," "Port Director," and "Seaport Security Assessment/Plan," stating that a seaport can act as its own legal entity and enforce its own laws and regulations.

As described in the temporary interim rule in part 101, Table 4 (68 FR 39266–39267), "area maritime," "port," and "port facility" are comparable, and we do not believe the recommended editorial changes add significant value or clarity. In addition, adding definitions incorporating "seaport," as suggested, is less inclusive than what is addressed in the MTSA. Furthermore, this concept does not align with the ISPS Code. We are not, therefore, amending parts 101 or 103.

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 "vitaly 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, we added a definition in part 101 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.

One commenter noted that in the definition of "transportation security incident," there should be a clear definition of the specific event or events the Coast Guard is trying to avoid or prevent, stating that for some of these events, industry already has good mitigation strategies in place that might avoid the need to add additional security measures.

The event that the Coast Guard is trying to avoid or prevent is a transportation security incident, which is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. As indicated in the

temporary interim rule (68 FR 39272) (part 101), we acknowledged that “many companies already have spent a substantial amount of money and resources to improve and upgrade security.” These improvements will be taken into account in their Vessel or Facility Security Assessments and subsequent security plan development.

One commenter suggested that the definition of “unaccompanied baggage” be revised to include baggage for which there is no accompanying passenger or crewmember. The commenter also noted that, if read literally, the definition in § 101.105 would include all passenger baggage already “checked,” and therefore separated from its owner. The suggested definition was the following: “baggage that was to be carried on board the ship when no passenger or crewmember was traveling on the same voyage or portion of that voyage.”

We agree that “unaccompanied baggage” should include baggage for which there is not an accompanying passenger or crewmember. With regard to “checked” baggage, our definition aligns with the ISPS Code, part B. “Checked” baggage at the point of inspection or screening should be with a crewmember or other person and therefore remains accompanied. After inspection or screening, the baggage will be controlled until it is loaded on the vessel. We have amended the definition of “unaccompanied baggage” to reflect the above and clarified the reference to an “other person.”

One commenter asked us not to change the definition of “vessel stores” as published in the temporary interim rule.

The definition of “vessel stores” remains the same as published in the temporary interim rule (68 FR 39281) (part 101).

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

We agree with the commenters. We have amended the definitions for “vessel-to-facility interface,” “vessel-to-port interface,” and “vessel-to-vessel

activity” in § 101.105 to use the words “cargo” and “vessel stores” instead of the word “goods” to be clearer for the intended activities. The term “vessel-to-facility interface” clearly states that the vessel is either at, or arriving at, the facility, and therefore, we did not amend the definition further.

Five commenters requested that we amend the definition of “waters subject to the jurisdiction of the United States” to simply refer to the definition of that term in 33 CFR 2.38, stating that doing so would be less confusing. Four commenters asked us to clarify the term “superadjacent” used in the same definition.

The definition suggested by the commenter would exclude application of these regulations to the Exclusive Economic Zone (EEZ) and waters superjacent to the OCS. We believe that including the EEZ and the waters superjacent to the OCS is crucial to implementing the comprehensive security regime intended by the MTSA. It is also consistent with the Coast Guard’s anti-terrorism authorities in 33 U.S.C. 1226. However, we agree the definition is somewhat confusing and needs clarification. In the temporary interim rules, we defined “waters subject to the jurisdiction of the United States” to include, in addition to the EEZ and the waters superjacent to the Outer Continental Shelf, the “navigable waters” as defined in 46 U.S.C. 2101(17a). Navigable waters in this context, by reference to Presidential Proclamation No. 5928, extend to the full breadth of the territorial sea that is 12 nautical miles wide, adjacent to the coast of the United States, and seaward of the territorial sea baseline. We believe the better approach is to amend our recent recodification of jurisdictional terms in 33 CFR part 2 to reflect that, consistent with the temporary interim rules, the 12 nautical mile territorial sea applies not only to statutes under subtitle II of title 46 but also statutes under subtitle VI of title 46 (section 102 of the MTSA). Doing so simplifies the definition of “waters subject to the jurisdiction of the United States” for purposes of the regulations by permitting reference, in part, to an existing regulatory definition. The amended definition of “waters subject to the jurisdiction of the United States” reflects this change.

Five commenters disagree with applying the same regulations to all segments of the maritime industry, stating that it is not practical. One of these commenters suggested that the regulations exempt entities, such as nuclear facilities covered under 10 CFR

part 73 and 49 CFR part 172, because they are already regulated.

We developed these regulations to be tailored to diverse industries within the maritime community through various provisions, such as the Alternative Security Program. If a nuclear facility is involved in the activities regulated under part 105, then the facility must comply with that part. However, we have made multiple provisions within the regulations so entities that are already covered by other requirements for security should be able to coordinate their compliance with these rules and others they already have implemented.

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 chapter I, 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."

Two commenters requested clarification on our reference to 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 Chapter I, 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 to the existing language.

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 final rules. We will review Alternative Security Program submissions in a timely manner to determine if they comply with the security regulations for their particular industry segment. The Coast Guard has already received and

begun reviewing Alternative Security Programs, and we have been able to approve three such programs. We have amended § 101.125 to list those approved Alternative Security Programs. We will announce new approvals of Alternative Security Programs through the **Federal Register**, and intend to update § 101.125 on an annual basis.

Twenty commenters requested clarification on the Alternative Security Program. Three commenters requested that the Coast Guard work with their industry association to come up with their own security program. Two commenters asked for guidance on how to implement an Alternative Security Program. One commenter stated that the Coast Guard should recognize its existing security programs. One commenter suggested that we allow owners or operators to use industry security standards, recommended practices, and guidelines as Alternative Security Programs. Four commenters requested that Alternative Security Programs be available to certain owners and operators of foreign flag vessels that are not subject to SOLAS. Three commenters asked for clarification as to which facilities are eligible to participate in an Alternative Security Program. One commenter recommended that the Alternative Security Program be available to vessels subject to SOLAS.

We encourage industries to develop Alternative Security Programs that address those aspects of security unique to their industry. Section 101.120 allows industry associations to submit Alternative Security Programs to the Coast Guard for approval. As part of the review process, we will work with industry representatives to assure that Alternative Security Programs meet the requirements of the rules and ensure maritime security. We agree that the Alternative Security Program should be available to certain owners and operators of foreign flag vessels that are not subject to SOLAS and to facilities that serve vessels on international voyages. Because the AMS Plan will be the approved port facility security plan as described in the ISPS Code, part A, we have amended § 101.120 to allow certain facilities that serve vessels subject to SOLAS Chapter XI the option of using an Alternative Security Program that has been reviewed and approved by the Coast Guard. We do not intend to allow vessels subject to SOLAS to use an Alternative Security Program. Two commenters stated that § 101.120 does not allow an industry association to submit an Alternative Security Program for approval. One commenter asked that the regulations

for Alternative Security Programs be clarified to allow participants to carry a copy of the Coast Guard approved Alternative Security Program on board vessels or at facilities.

Section 101.120(c) does not preclude an industry association from submitting an Alternative Security Program for approval. In addition, the regulations requiring the availability of the security plans on board the vessels or at the facility do not preclude the owner or operator of the vessel or facility from keeping a Coast Guard approved Alternative Security Program on board the vessel or at the facility. Furthermore, we have amended § 101.120(b)(3) and added a new provision, § 101.120(b)(4), to clarify that owners or operators implementing an Alternative Security Program must provide information to the Coast Guard when requested. This clarification was needed, among other things, to ensure that the Coast Guard has access to relevant information to assist our compliance and verification responsibilities. The information may also be needed to help the Coast Guard assess vulnerabilities, conduct an AMS Assessment, or develop an AMS or National Security Plan. Finally, after further review of parts 101 and 104 through 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 Plan, and it must be readily available.

Three commenters stated that the cognizant COTP should be responsible for reviewing the submissions for the Alternative Security Program when the company operates exclusively in one COTP zone. The commenters noted that COTPs have the best knowledge of the vessels and facilities operating in their zone.

We require that requests to implement an Alternative Security Program be submitted for approval to the Commandant (G-MP) because we want to ensure uniformity across all COTP zones in the implementation of this program. The Commandant (G-MP) will coordinate and consult with local COTPs, Districts, and Areas, as needed, on these submissions.

After further review of § 101.120, we are amending the section to provide a procedure for amending an Alternative Security Program, and to align the effective period of an Alternative Security Program with the 5-year period provided for other security plans. Additionally, after 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 seven comments regarding waivers, equivalencies, and alternatives. Three commenters appreciated the flexibility of the Coast Guard in extending the opportunity to apply for a waiver or propose an equivalent security measure to satisfy a specific requirement. Four commenters requested detailed information regarding the factors the Coast Guard will focus on when evaluating applications for waivers, equivalencies, and alternatives.

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

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

We do not agree with adding a definition of “port” to recognize a group of facilities that combine to act as an identified unit. However, groups of facilities may work together to enhance their collective security and achieve the performance standards in the regulations. Locally developed port security plans may serve as an excellent starting point for those facilities located within the jurisdiction of a port authority. We believe that the provisions of §§ 105.300(b), 105.310(b), and 105.400(a) permit the COTP to approve a Facility Security Plan that covers multiple facilities, such as a co-located group of facilities that share security arrangements, provided that the

particular aspects and operations of each subordinate facility are addressed in the common assessment and security plan. A single Facility Security Officer for the port or cooperative should be designated to facilitate this common arrangement. Finally, local security programs developed by entities such as a port authority or a port cooperative may be submitted to the Coast Guard for consideration as Alternative Security Programs in accordance with § 101.120(c).

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

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

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

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

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

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

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

Subpart B—Maritime Security (MARSEC) Levels

This subpart concerns the setting of MARSEC Levels.

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

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

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

Subpart C—Communication (Port-Facility-Vessel)

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

suspicious activities, breaches of security, and transportation security incidents.

We received 28 comments regarding communication of changes in the MARSEC Levels. Most commenters were concerned about the Coast Guard's capability to communicate timely changes in MARSEC Levels to facilities and vessels. Some stressed the importance of MARSEC Level information reaching each port area in the COTP's zone and the entire maritime industry. Some stated that local Broadcast Notice to Mariners and MARSEC Directives are flawed methods of communication and stated that the only acceptable means to communicate changes in MARSEC Levels, from a timing standpoint, are via 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 means. Communication of MARSEC Levels will be done in the most expeditious means available, given the characteristics of the port and its operations. These means will be outlined in the AMS Plan and exercised to ensure vessel and facility owners and operators, or their designees, are able to quickly communicate with us and vice-versa. Because MARSEC Directives will not be as expeditiously communicated as other COTP Orders and are not meant to communicate changes in MARSEC Levels, we have amended § 101.300 to remove the reference to MARSEC Directives. We have added a reference to electronic means.

One commenter suggested that major commodity groups, including the chemical, hazardous material, utility, rail, truck, and air transportation industries receive information regarding potential threats from the local COTP.

As stated in § 101.300(b), the COTP will, when appropriate, communicate to port stakeholders certain information regarding known threats that may cause a transportation security incident.

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 is 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) 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.

One commenter asked whether the COTP's communication of required actions to minimize risk, under § 101.300(b)(5), refers only to measures that have been detailed in the Vessel Security Plan or the Facility Security Plan.

At any MARSEC Level, the COTP, consistent with the authority in 33 U.S.C. chapter 1221 and 50 U.S.C. chapter 191, may require owners and operators to take measures to counter security threats that are beyond those detailed in their security plans when necessary to prevent injury or damage or to secure the rights and obligations of the U.S. This is consistent with requirements specified in the ISPS Code.

We received 19 comments on the requirements that owners and operators of vessels and facilities confirm attainment of increased MARSEC Level security measures. Some requested that the Master, not the owner or operator, be responsible for reporting to the local COTP the attainment of the change in MARSEC Level. Several commenters sought clarification as to which COTP they need to report their attainment of security measures. Others questioned the ability of the COTP to receive potentially hundreds of calls confirming attainment of security measures in their security plan or requirements imposed by the COTP. Finally, some questioned the benefit of reporting compliance with the MARSEC Level change.

We agree with the comment to allow owners and operators to designate the

Master or another appropriate person to be responsible for reporting the attainment of the MARSEC Level and are amending § 101.300 to allow this. Our intent is to have one company representative contact the local COTP to minimize the number of calls to the local COTP during a change in MARSEC Level. Consistent with the ISPS Code, part A, attainment measures should be reported to the COTP that issued the notice of the change in MARSEC Levels to that vessel, so as to ensure compliance.

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 to effectively coordinate the implementation of security measures. Thus, we have placed this requirement on the owner or operator, not the Coast Guard. The Coast Guard will be inspecting facilities and vessels to ensure this communication is accomplished.

Twelve commenters requested that the Coast Guard issue specific communications guidelines to affected facilities and vessels bound for and operating in U.S. ports. One commenter stated that, in guidance, we should define a means by which changes in MARSEC Levels will be communicated to U.S. flag vessels that are not in the coastal waters.

We recognize that further guidance should be provided to ensure communication expectations are clearly outlined. We intend to update the guidance in NVIC 9-02 (Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports) to address communications with facilities and vessels bound for and operating in U.S. ports. We will also address communication of MARSEC Levels with U.S. flag vessels operating internationally in this guidance and intend to coordinate these types of communications with MARAD.

Two commenters suggested web-based information sharing methods. One commenter recommended a proprietary, secure, web-based information portal for vessels, port facilities, and other transportation/supply chain participants to report and record required security information, security documents, and security checks in complying with Coast

Guard and IMO requirements. One commenter suggested that the Coast Guard include information to coordinate and provide access to regulatory compliance tools on a website. The commenter also suggested that the preamble accompanying the final rules should have well-named headings to assist the regulated community in locating information, including language explaining the applicability of SOLAS and including a list of contracting governments.

We intend to be flexible in the implementation of communication reporting methods to be used by vessel and facility owners or operators, and we are working on a website to provide security information to the regulated community. We encourage owners or operators to implement a system that best allows them to meet the reporting and recordkeeping requirements of their approved security plan. Additionally, the Coast Guard has provided headings throughout this preamble, based on the subparts of these security rules, to assist the public in locating information. SOLAS applicability is clearly defined in SOLAS and IMO maintains a list of contracting governments, which can be found on IMO's website (<http://www.imo.org>).

Twenty commenters made suggestions regarding reporting to the National Response Center (NRC) under § 101.305. Five commenters did not support notification to the NRC for all breaches of security. Two commenters stated that because the scope of the term "transportation security incident" and the meaning of the terms "may result" and "breach of security" are not clear, the regulated community is at risk of both over-reporting and under-reporting suspicious activity. Three commenters also suggested that the Coast Guard make a distinction between suspicious activities and an actual transportation security incident. Four commenters stated that it is not clear what the NRC would do with the information about suspicious incidents or how such a notification would sufficiently improve facility security in concert with other reporting processes for suspicious activity or security incidents. Eight commenters suggested that notifying the NRC "without delay" will not provide for the quickest response and suggested that owners or operators be allowed to: (1) Activate the security plan; (2) notify local law enforcement; (3) notify the local COTP; (4) use VHF channel 16 to notify the local area; or (5) notify the NRC "as soon as practical."

The Coast Guard provided a distinction between suspicious activities and a transportation security

incident in part 101. A "transportation security incident" is defined in § 101.105, as "a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area." As stated in § 101.305(a), a "suspicious activity" is an activity that may result in a transportation security incident. The purpose of requiring vessel and facility owners or operators to report suspicious activities or breaches of security "without delay" to the NRC is to enable the Coast Guard to identify patterns of this type of activity on a national scale and consult with other Federal agencies to confirm if the activity is a coordinated threat to our nation. The NRC will also relay to the COTP, and as appropriate port stakeholders, vessels, and facilities, reports of suspicious activities, breaches of security, and information concerning security-related patterns and trends. Because it is imperative to identify nationwide threat patterns, we did not amend the reporting requirements for suspicious activities or breaches of security. In the case of a transportation security incident, the notification goes, without delay, to the COTP or cognizant District Commander for OCS facilities, because of the need to assess impacts to the port area and to implement the AMS Plan, as appropriate.

Subpart D—Control Measures for Security

This subpart concerns control and compliance measures, including enforcement, MARSEC Directives, and penalties.

Seventeen commenters urged the Coast Guard to fully recognize the need for consistency in the application and enforcement of security-related regulations and in the plan approval process across several COTP zones.

We do recognize the need for consistency in the application and enforcement of the regulations. Therefore, the Coast Guard will continue to develop guidance for COTPs to consistently implement and enforce the security regulations.

Two commenters stated that the "entire issue of the authority to issue a MARSEC Directive" needed clarification. In addition, the commenters noted that in § 101.405(a)(1), the Commandant may delegate the authority to issue MARSEC Directives and indicated that this authority should remain with the Commandant.

MARSEC Directives are necessary as a mechanism to provide specific instruction to achieve the performance

standards required by these regulations and 46 U.S.C. Chapter 701 but that should not be open to the general public. As such, the MARSEC Directives will be labeled as sensitive security information because they will contain information that, if disclosed, could be used to exploit security systems and measures. MARSEC Directives will be issued under an extension of the Coast Guard's existing COTP authorities regarding maritime security, found in 33 U.S.C. 1226 and 50 U.S.C. 191. In part, the implementing regulations for 50 U.S.C. 191, found at 33 CFR 6.14-1 and promulgated by Executive Order 10277, contemplate action by the Commandant that is national in scope. Specifically, these regulations authorize the Commandant to prescribe such conditions and restrictions deemed necessary under existing circumstances for the security of certain facilities or public and commercial structures and vessels. Additionally, 43 U.S.C. 1333(d) authorizes the Coast Guard to establish certain requirements for OCS facilities. Moreover, MARSEC Directives are a necessary and integral part of carrying out the Coast Guard's authorities in 46 U.S.C. Chapter 701. The Commandant, at this time, intends to retain the authority to issue all MARSEC Directives.

Forty-three commenters requested clarification on issuance and receipt of MARSEC Directives. Several suggested that the Coast Guard: allow companies to submit a national "security sensitive information form," rather than notifying each COTP that companies have a "need to know" the security sensitive information contained in MARSEC Directives; have MSOs make Directives from all other MSOs available, which will allow them to have "1-stop shop" service; and, develop a secure website where individuals with sensitive security information authorization could access directives from all COTP zones. Many stated that owners and operators should not be required to comply with MARSEC Directives if they cannot or are not allowed to access the information in the Directive when that information is sensitive security information. Some were concerned that owners and operators would not know if they had a "need to know" the information in a MARSEC Directive under § 101.405(a)(2). Several comments asked for clarification of who will be granted access to applicable MARSEC Directives. One commenter requested a standardized process for applying for "need to know" status. One commenter argued that proof of a "need to know" undermines the purpose of

communicating MARSEC Directives. One commenter said there should be one U.S. agency responsible for disseminating non-classified security information to shippers who do not have security clearances. Some commenters asked if vessel agents would be able to obtain copies of a MARSEC Directive on behalf of the vessel owner or operator. Most stated that the current process for communicating MARSEC Directives is cumbersome and suggested the best practice to inform foreign vessels entering waters under the jurisdiction of the U.S. would be to notify each at the time they file their 96-hour Notice of Arrival.

We recognize that the MARSEC Directive provision in § 101.405 establishes a challenging process for distributing directives to the regulated community. To ensure nationwide consistency, MARSEC Directives are issued at the Commandant level and, therefore, will allow each MSO to serve as a "1-stop shop" for MARSEC Directives. When owners, operators, or appointed agents of an owner or operator are notified of a MARSEC Directive, information will be included indicating those that have a "need to know." To verify that an owner or operator has the "need to know" the content of a MARSEC Directive, MSOs have several tools available to them, including a database of vessels and facilities and their owner and operator information. In addition, an MSO can determine if a Company Security Officer, Vessel Security Officer, or Facility Security Officer has a "need to know" if an approved Vessel Security Plan or Facility Security Plan is presented to them. Once a person has provided enough information for the MSO to verify that person's "need to know" and status as a regulated entity, the MSO will provide the MARSEC Directive. The "need to know" designation is required to protect sensitive security information from being exploited. We also recognize that further guidance should be provided to ensure communication expectations are clearly outlined and intend to update the guidance in NVIC 9-02 (Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports) to address distribution of MARSEC Directives.

One commenter asserted that there needs to be a means for industry and stakeholders to provide input or feedback both before and after the MARSEC Directive becomes effective, considering their knowledge of what will or will not work in an effective shipboard security program.

The regulations, in § 101.405, currently limit the authority to issue MARSEC Directives to the Commandant or his/her designee; however, we intend to consult other Federal agencies having an interest in the subject matter prior to issuing MARSEC Directives. When appropriate and as time permits, we intend to further consult with the affected industry. Section 101.405(d) also provides for an owner or operator to propose equivalent security measures in the event that they are unable to comply with MARSEC Directives.

Two commenters anticipated that MARSEC Directives would be prescriptive and that the Coast Guard should grant alternatives and equivalencies under these Directives. One commenter asked whether a recipient of a MARSEC Directive can maintain equivalent security measures for the duration of the directive, which could be open-ended, or if the recipient would have a certain amount of time to specifically comply with the MARSEC Directive.

We agree that there should be opportunities for owners and operators to implement alternatives or equivalent security measures to those prescribed in a MARSEC Directive. We provided these opportunities in § 101.405, which governs § 104.145 (MARSEC Directives), to allow equivalent security measures to be submitted to the Coast Guard in lieu of the specific measures required in a MARSEC Directive. Equivalencies approved by the Coast Guard under a specific MARSEC Directive will be in effect for the duration of that Directive.

Two commenters stated that our regulations suggest that information designated as sensitive security information is exempt from the Freedom of Information Act (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.

Three commenters stated that § 101.405(a)(2) refers to a "covered

person" as a term defined in 49 CFR 1520 related to sensitive security information. However, upon review of those regulations, they did not find a definition of "covered person" in those regulations.

We agree that the terminology in § 101.405(a)(2) is confusing. Therefore, we are clarifying § 101.405(a)(2) by amending the phrase "require owners or operators to prove that they have a 'need to know' the information in the MARSEC Directive and that they are a 'covered person'" to read "require the owner or operator to prove that they are a person required by 49 CFR 1520.5(a) to restrict disclosure of and access to sensitive security information, and that under 49 CFR 1520.5(b), they have a need to know sensitive security information."

One commenter suggested that we amend § 101.405 and change the words "may" and "should" to read "will" and "shall."

We do not believe the recommended editorial changes add significant value or clarity.

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

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

Two commenters stated that in its control and compliance measures, the Coast Guard should clarify its legal authority to establish a security zone beyond its territorial sea.

One basis for the Coast Guard to establish security zones in the EEZ is pursuant to the Ports and Waterways Safety Act, 33 U.S.C. 1221 *et seq.* For

example, consistent with customary international law, 33 U.S.C. 1226 provides the Coast Guard with authority to carry out or require measures, including the establishment of safety and security zones, to prevent or respond to an act of terrorism against a vessel or public or commercial structure that is located within the marine environment. 33 U.S.C. 1222 defines "marine environment" broadly to include the waters and fishery resources of any area over which the U.S. asserts exclusive fishery management authority. The U.S. asserts exclusive fishery management authority in the EEZ.

Ten commenters were concerned that the control and compliance measures section did not address the liability implications of implementing the provisions required by these regulations and complying with the directives associated with the MARSEC Levels established by the Coast Guard. Two commenters were concerned with the liability for oil spills resulting from a transportation security incident. Two commenters recommended that the strict liability scheme under OPA 90 not be used for such circumstances. Two commenters believed there is a need to address liability for undue delay during application of control measures. One commenter believed there is a need to address Coast Guard liability in the context of owners or operators acting as government agents when conducting screenings. One commenter questioned whether the ship agent, whose bond is often used for Customs clearance for a vessel, would be liable if a vessel violates control and compliance issues.

An approved security plan under these security regulations satisfies the requirements of 46 U.S.C 70103(c)(3)(D). The fact that a transportation security incident is not deterred does not alone constitute a failure to comply with these security regulations. Failure to follow the approved plan, however, is a violation of these regulations. While we appreciate the points raised concerning potential liability for terrorist acts and when owners or operators are conducting screenings, the issue of liability is beyond the scope of this final rule. No provision of the MTSA addressed liability, either to expressly limit liability or to address immunity from liability. Additionally, the MTSA did not address liability within the context of undue delay. Among other things, determinations of liability require a fact-laden inquiry on a case-by-case basis and typically require complex analyses regarding matters such as choice of law, contracts, and international conventions. Undue delay is a term used in international

conventions and likewise requires fact-laden analysis that we leave for the courts. We note that OPA 90 provides three defenses to its liability regime (act of God, act of war, or act or omission of a third party, as set forth 33 U.S.C. 2703). Whether one of these defenses will apply to a transportation security incident will depend on the facts of each case. Concerning the comment regarding compensation for undue delay of vessels, we note that this is a principle commonly found in IMO instruments, including other parts of SOLAS and the International Convention for the Prevention of Pollution from Ships, 1973, as modified by the Protocol of 1978 relating thereto (MARPOL 73/78). Therefore, we anticipate that claims for undue delay under SOLAS Chapter XI-2, regulation 9, will be resolved similar to the resolution found in these other instruments.

One commenter said that penalties should be applied equally to both U.S. flag vessels and foreign flag vessels.

We believe that the commenter misunderstood the nature of authorities granted to port and flag states. The assertion that penalties are applied unequally to U.S. and foreign flag vessels is incorrect. Civil penalties authorized by 46 U.S.C. 70117 apply equally to both U.S. and foreign vessels that do not meet the requirements of the regulations. Because we can revoke, at any point, ISSCs for Vessel Security Plans that we approve, we have full discretion in enforcing the rules on those vessels. For foreign flag vessels whose ISSCs are issued by its flag administration, we can enforce the regulations by not allowing the vessel to call at our ports, or we can work with the country issuing the vessel's ISSC to revoke it. We will enforce the regulations equally; however, the comment brought to light the need to clarify § 101.410(b)(8) to include the right of the U.S. to revoke any security plan we approve, and we have amended the section to clarify this requirement.

After reviewing § 101.420, we amended paragraph (b) to clarify that appeals of certain decisions and actions of the District Commander should be made to the Commandant (G-MOC).

Subpart E—Other Provisions

This subpart concerns Declarations of Security, security assessment tools, and credentials for personal identification.

Three commenters stated that the Coast Guard should delegate its authority for reviewing and approving security plans to an RSO, stating that if the Coast Guard reviews and approves

all plans, this will interfere with other critical Coast Guard missions.

We believe that it is imperative to maritime homeland security to ensure consistent application of the requirements of parts 101 through 106 and will conduct the reviews and approvals of certain security plans. We do not intend to delegate authority to an RSO at this time. Reconsideration and further delegation of plan approvals may be provided once a stable nationwide foundation for maritime security has been established. Although the Coast Guard is not delegating plan approval authority, we have ensured plan review resources will be sufficient for implementing these regulations while not negatively affecting Coast Guard missions.

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 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 asked whether the Declaration of Security requirement applies to vessel-to-vessel or vessel-to-facility interfaces beyond the 12-mile limit but still in the U.S. EEZ.

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

We received 15 comments regarding security assessment tools. Eleven commenters would like the Coast Guard to formally approve a separate security assessment methodology as one that may be used by a refiner or petrochemical manufacturer, and also to incorporate it by reference. The commenters believe that it is a sophisticated and effective methodology for conducting Facility Security Assessments. One commenter asked whether an owner or operator who has

already completed a risk assessment using a risk assessment tool other than those listed in § 101.510 must conduct a new assessment using one of those tools. Three commenters asked that the Coast Guard provide a list of security assessment tools that would satisfy all DHS and Coast Guard requirements.

The Coast Guard does not intend to approve security assessment tools or incorporate such tools by reference because we prefer to allow flexibility for industry to develop their own tools to meet their specific needs. We have provided a list of examples of security assessment tools in § 101.510; however, this list is not exhaustive. We do not require owners or operators to conduct security assessments using these tools as long as the assessments meet the requirements of these regulations. To clarify that the list in § 101.510 represents some, but not all, assessment tools available for facilitating security assessments, we have amended it to include the word "may."

It should be noted that the list in § 101.510 includes a no-cost, user-friendly, web-based, vulnerability-self-assessment tool designed by TSA. This tool was developed by TSA in coordination with other Federal agencies and members of academia and industry as a means to assist vessel and facility owners and operators in completing the security assessments mandated by these maritime security regulations. Any information entered into the tool will not be accessible by TSA or any other Federal agencies unless the owner or operator formally submits this information to TSA. TSA, in coordination with the Coast Guard, is developing guidance that will assist users of the TSA tool. At this time, TSA does not intend to publish a Notice of Proposed Rulemaking requiring the use of this tool.

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 the temporary interim rule requirement to institute a photo identification card system for crewmembers is unreasonable because it will cost over \$2,000 and will be obsolete when the Transportation Worker Identification Credential (TWIC) requirement is enacted. One commenter stated that some ports are already establishing credentialing programs of varying complexity and scope and emphasized the need for the national TWIC program to be implemented as soon as possible.

The temporary interim rule does not require vessel or facility owners or operators to have a photo identification card system that is vessel or facility specific. The personal identification requirements of § 101.515 are well within the scope of the majority of current identification systems such as driver's licenses and union cards. Vessel and facility owners or operators can use any personal identification that meets the requirements of § 101.515; they do not have to develop their own card systems. Section 101.515 was meant to provide a temporary solution to the criteria for personal identification to facilitate access control until the TWIC criteria could be implemented. TSA is working closely with other agencies of DHS (e.g., the Coast Guard), agencies of DOT (e.g., MARAD), and other government agencies to develop the TWIC and its use to ensure that it can be a practical personal identification system for the transportation community.

Two commenters stated that our regulations will require employers to reissue identification cards when individuals grow beards or mustaches because the photo will not "accurately depict the individual's current facial appearance."

Facial hair may not necessarily alter the depiction of an individual on picture identification so much that the individual is no longer identifiable. If the individual depicted on the identification has changed his or her appearance to the extent that the individual is no longer accurately depicted, then a new identification card would be required.

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

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

After further review, and based on comments from several other agencies and Coast Guard field units, 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.

Two commenters stated concerns regarding standards for seafarers' identification cards and other identifying documents. One commenter stated that the Coast Guard must ensure

that foreign and U.S. requirements for seafarers' identification are consistent. The commenter also stated that the Coast Guard must ensure consistency among U.S. facilities. One commenter urged the Coast Guard to provide a comprehensive and clear explanation of whether the U.S. will be using the new ILO seafarers' identity documents.

We appreciate the commenters' concern regarding standards for seafarers' identification cards and the intentions of the U.S. with regard to international seafarers' identity documents, but these comments are beyond the scope of these rules. We have provided minimum requirements for determining whether an identification credential may be accepted in § 101.515. We also discussed, in detail, our intentions regarding seafarers' identification criteria in the preamble to the "Implementation of National Maritime Security Initiatives" temporary interim rule (68 FR 39264).

One commenter supported making foreign-flag shipowners, operators, and ship managers responsible for establishing a vetting program of their newly hired officers and crew, requiring background checks of their seafarers, and having the Coast Guard audit those firms to ensure the vetting is done. The commenter stated that having a system for vetting would eliminate a "loophole" that could result in loss of American lives and property.

We will continue a vigorous Port State Control program that will now include verifying compliance with SOLAS and the ISPS Code for foreign-flag SOLAS vessels. We have been working aggressively, both internationally and nationally, to develop seafarer's identification requirements that include the vetting of newly hired officers and crew and that also address background check requirements. Since the implementation of the International Safety Management Code (ISM Code), audits and other quality verifications are now standard in the international maritime community. Therefore, once a seafarer's identification requirement is established, we expect it will be audited under the ISM Code, and foreign flag vessels will not require specific Coast Guard oversight.

One commenter stated that part 102 provisions in the temporary interim rule should make the seafarers' identification documents that comply with ILO-185 acceptable as a substitute for or waiver of a visa for shore leave.

Part 102 has been reserved for the National Maritime Transportation Security Plan, not seafarers' identification. Section 101.515

addresses identification. The requirements in § 101.515 are not waivers for a visa. Visas are a matter of immigration law and are beyond the scope of these final rules.

Part 102—National Maritime Transportation Security

This part is reserved and concerns the development of the overarching National Maritime Transportation Security Plan for sustaining National Maritime Security initiatives.

Procedural

Fourteen commenters addressed the public comment period. One commenter stated that another comment period will be necessary once plans are approved. Six commenters said the 30-day comment period was inadequate and should be lengthened. Five commenters requested a longer comment period specifically for the AIS temporary interim rule.

We did not extend the comment period due to the need to follow the MTSA's statutory deadline for issuance of regulations. We acknowledge that these regulations are being implemented in a short period of time. In this final rule, we require security measures, assessments, and plans for those vessels and facilities we have determined may be involved in a transportation security incident. It is not clear how further comments will benefit security after plan submission is complete. We continually review guidance we issue to implement regulations and welcome feedback on guidance we have developed for these regulations. Regarding AIS specifically, we will be reopening the comment period on our previously published notice titled "Automatic Identification System; Expansion of Carriage Requirements for U.S. Waters" (USCG 2003-14878; July 1, 2003; 68 FR 39369).

Three commenters addressed the public meeting held on July 23, 2003. One commenter asked the Coast Guard to hold an additional public meeting in the Houston, Texas, area and proposed several dates in July 2003. Two commenters stated that many came to the public meeting believing that it would be not just a listening session, but also an opportunity to discuss and clarify the proposed regulations, in preparation for submitting written comments before the end of the comment period.

We acknowledge that these regulations are being implemented in a short period of time. Due to the time constraints of the MTSA, however, we held only one public meeting on July 23, 2003. Previous public meetings in

January 2002 and in January and February 2003 provided the public several opportunities to discuss various maritime security issues with Coast Guard representatives. Because the opportunity to hear public comments is so important, we set an agenda for the July 2003 meeting that allowed us to hear public comments rather than to debate the issues further. Additionally, the preambles to the temporary interim rules clearly stated our position on maritime security, which did not need further elucidation in a public setting at the expense of receiving stakeholders' comments.

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. In addition, the part heading in this part has been amended to align it with all the part headings within this subchapter.

Incorporation by Reference

The Director of the Federal Register has approved the material in § 101.115 for incorporation by reference under 5 U.S.C. 552 and 1 CFR part 51. Copies of the material are available from the sources listed in § 101.115.

This final rule incorporates by reference SOLAS Chapters XI-1 and XI-2 and the ISPS Code. Specifically, we are incorporating the amendments adopted on December 12, 2002, to the Annex to SOLAS and the ISPS Code, also adopted on December 12, 2002. The material is incorporated for all of subchapter H. The final rule titled "Automatic Identification System; Vessel Carriage Requirement" (USCG-2003-24757), found elsewhere in today's **Federal Register**, has its own incorporation by reference section in 33 CFR 164.03.

Regulatory Assessment

This final rule is a "significant regulatory action" under section 3(f) of Executive Order 12866, Regulatory Planning and Review. The Office of Management and Budget has reviewed it under that Order. It requires an assessment of potential costs and benefits under section 6(a)(3) of that Order. It is significant under the regulatory policies and procedures of the Department of Homeland Security. A summary of comments on the assessments, our responses, and a summary of the assessments follow.

We received 11 comments relating to the cost of implementing these regulations. Nine commenters asked if DHS plans to offer annual grants to

assist in covering the costs incurred by the operators to satisfy the requirements of the rules. Two commenters stated that compliance with all security requirements should be extended to 2008, or until sufficient monies are allocated by the Congress to cover cost. One commenter stated that the regulations should grant enough flexibility to COTPs to consider a facility's limited resources and cost-effectiveness ratio of implementation when they review the security plan for approval. Three commenters asked how these rules recognize and assist very small ports and small businesses.

We appreciate that the cost of implementing these regulations could have significant impacts on annual revenues for some vessel or facility owners and operators. Pursuant to Section 102 of the MTSA, DOT is required to develop a grant program. DHS is working with DOT on the grant program. At this point, we do not know if Congress will appropriate funds to continue this program and allow for grants on a continuing annual basis. We cannot alter the compliance dates of these regulations because they are mandated by the MTSA and aligned to meet the entry into force date of SOLAS Chapter XI and the ISPS Code. We recognize the difficulty small facilities may have in meeting our security requirements and, therefore, we have developed flexible measures and performance-based standards to allow owners or operators to implement cost-effective security measures. We have made the requirements as flexible as possible and have analyzed the risk to ensure that applicability is focused on those vessels and facilities that may be involved in a transportation security incident.

Two commenters addressed the burdens involved in moving from MARSEC Level 1 to MARSEC Level 2. One commenter 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 DHS to ensure 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; however, it is only one of several MARSEC Level 2 security enhancements listed in § 105.255(f), which is not an exclusive list.

Three commenters stated that security measures required under MARSEC Level 3 would pose an unfair economic burden upon an owner or operator and could create an "industry" for additional security measures.

The security measures required under MARSEC Level 3 are designed to address the increased threat of a probable or imminent transportation security incident. At this highest level of threat, the maritime industry is vulnerable to a transportation security incident and can be exposed to significant economic losses. Were a maritime transportation security incident to occur, the nation could experience devastating losses, including significant loss of life, serious environmental damage, and severe economic shocks. While we can reasonably expect MARSEC Level 3 to increase the direct costs to businesses attributable to increased personnel or modified operations, we believe the indirect costs to society of the "ripple effects" associated with a transportation security incident would greatly outweigh the direct costs to the maritime industry. Additionally, we expect this highest level of threat to occur infrequently.

Five commenters stated that our cost estimates understate the cost for international ships calling on U.S. ports. Three commenters noted that the same parameters used to develop the costs for the U.S. SOLAS vessels should be extrapolated and applied to international ships, adjusted for the

time these ships spend in waters subject to the jurisdiction of the U.S. One commenter asked us to explain why only 70 foreign flag vessels were included in our analysis of the cost of the temporary interim rule.

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

One commenter suggested 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 are available in the dockets for both the temporary interim rules and the final rules, and they account for companies as whole business entities, not individual vessels or facilities.

One commenter was concerned that the entire list of ships that are directly regulated under part 104 have been designated as "high risk" for a transportation security incident. The commenter noted that no account appears to have been taken of the different types of vessels or specific threats and warnings.

We explained in detail in the temporary interim rule (68 FR 39244-6) (part 101) how we used the National Risk Assessment Tool (N-RAT) to determine risks associated with specific

threat scenarios against various classes of targets within the MTS.

Two commenters questioned the accuracy of the estimated average fatalities from a transportation security incident for a large passenger vessel. One commenter reasoned that the “outstanding” safety record of the industry in recent history does not substantiate the estimated average fatalities for an accident and, therefore, puts into question our estimated average fatality for a transportation security incident. One commenter urged caution in interpreting figures between safety and security to determine what is a transportation security incident.

Our initial estimated number of fatalities on large passenger ships was based on major maritime accidents over the past century. We noted that historically, the worst maritime accidents (*e.g.*, Titanic, Lusitania, Empress of Ireland) produced fatality rates over 50 percent. However, the commenter is correct in asserting that portions of the large passenger vessel industry have experienced a significant period of time with few accident-related fatalities which can be attributed, in part, to innovations in safety and advances in accident survivability. Therefore, since the dataset used to compile the estimated number of fatalities per accident lacked recent events, we used the lower estimate of 32 percent, which is based on the actual fatality rate of accidents involving small passenger vessels. We acknowledge that small passenger vessels would likely use different safety and survivability measures than large passenger vessels. However, we disagree that using the 32 percent for the estimated average accident-related fatality rate for large passenger vessels is incorrect—it illustrates a catastrophic failure. The estimated average fatality rate for a transportation security incident is higher than for a safety-related accident because a transportation security incident is perpetrated with the intent to inflict a high casualty rate. Safety measures, therefore, will have some, but not an equivalent level of effectiveness during a transportation security incident. We believe that the average transportation security incident-related fatality rate, in general for those directly regulated under subchapter H, and in particular for large passenger vessels, will result in a “significant loss of life” and, therefore, be a transportation security incident.

One commenter asked for clarification on whether the N-RAT results indicated a lower risk for facilities that do not receive vessels on international voyages, even if those voyages are by vessels

exceeding 100 gross tons and transiting international waters. The commenter also asked whether Guam and the Northern Marianas Islands are part of the U.S. and whether a domestic voyage may cross international waters.

The N-RAT indicated that vessels on international voyages may be involved in a transportation security incident. In § 101.105, the term “territory” includes the Commonwealth of Puerto Rico, all possessions of the U.S., and all lands held by the U.S. under a protectorate or mandate. This includes Guam and the Northern Marianas Islands. A domestic voyage includes a direct transit between two U.S. ports, regardless of whether the vessel transits international waters.

One commenter asked if there is any public benefit to building infrastructure and increasing staffing, stating that the ports have no way to pay for such upgrades.

Using the N-RAT, we determined that significant public benefit accrues if a transportation security incident is avoided or the effects of the transportation security incident can be reduced. These public benefits include human lives saved, pollution avoided, and “public” infrastructure, such as national landmarks and utilities, protected.

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 assessment 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 assessment 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.

Cost Assessment Summary

The following summary presents the estimated costs of complying with the final rules on Area Maritime Security, Vessel Security, Facility Security, OCS Facility Security, and AIS, which are published elsewhere in today’s **Federal Register**. Because the changes in this final rule do not affect the original cost

estimates presented in the temporary interim rule (68 FR 39272) (part 101), the costs remain unchanged.

For the purposes of good business practice, or to comply with 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 summary do not include the security measures that these companies have already taken to enhance security.

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

This assessment presents the estimated cost if vessels, facilities, OCS facilities, and areas are operating at MARSEC Level 1, the current level of operations since the events of September 11, 2001. We also estimate the costs for operating for a brief period at MARSEC Level 2, an elevated level of security. We also discuss the potential effects of operating at MARSEC Level 3, the highest level of threat.

We do not anticipate that implementing the final rules will require additional manning aboard vessels or OCS facilities; existing personnel can assume the duties envisioned. For facilities, we anticipate additional personnel in the form of security guards that can be hired through contracting with a private firm specializing in security.

Based on our assessment, the first-year cost of implementing the final rules is approximately \$1.5 billion.

Following initial implementation, the annual cost is approximately \$884 million, with costs of present value \$7.331 billion over the next 10 years (2003–2012, 7 percent discount rate). Estimated costs are as follows.

Vessel Security

Implementing the final rule will affect about 10,300 U.S. flag SOLAS, domestic (non-SOLAS), and foreign non-SOLAS vessels. The first-year cost of purchasing and installing equipment, hiring security officers, and preparing paperwork is approximately \$218 million. Following initial implementation, the annual cost is approximately \$176 million. Over the

next 10 years, the cost would be present value \$1.368 billion.

Facility Security

Implementing the final rule will affect about 5,000 facilities. The first-year cost of purchasing and installing equipment, hiring security officers, and preparing paperwork is an estimated \$1.125 billion. Following initial implementation, the annual cost is approximately \$656 million. Over the next 10 years, the cost would be present value \$5.399 billion.

OCS Facility Security

Implementing the final rule will affect about 40 OCS facilities under U.S. jurisdiction. The first-year cost of purchasing equipment and preparing paperwork is an estimated \$3 million. Following initial implementation, the annual cost is approximately \$5 million. Over the next 10 years, the cost would be present value \$37 million.

Area Maritime Security

Implementing the final rule will affect about 47 COTP zones containing 361 ports. The initial cost of the startup period (June 2003–December 2003) is estimated to be \$120 million. Following the startup period, the first year of implementation (2004) is estimated to be \$106 million. After the first year of implementation, the annual cost is approximately \$46 million. Over the next 10 years, the cost would be present value \$477 million.

Automatic Identification System (AIS)

Implementing the final rule will affect about 3,500 U.S. flag SOLAS vessels, domestic (non-SOLAS) vessels in Vessel Traffic Service (VTS) areas, and foreign flag non-SOLAS vessels. The first-year cost of purchasing equipment and training for U.S. vessels (SOLAS and domestic) is approximately \$30 million. Following initial implementation, the annual cost is approximately \$1 million. Over the next 10 years, the cost for these vessels would be present value \$50 million (with replacement of the units occurring 8 years after installation).

MARSEC Levels 2 and 3

MARSEC Level 2 is a heightened threat of a security incident, and intelligence indicates that terrorists are likely to be active within a specific target or class of targets. MARSEC Level 3 is a probable or imminent threat of a security incident. MARSEC Levels 2 and 3 costs are not included in the above summaries because of the uncertainty that arises from the unknown frequency of elevation of the MARSEC Level and the unknown duration of the elevation.

The costs to implement MARSEC Levels 2 and 3 security measures in response to these increased threats do not include the costs of security measures and resources needed to meet MARSEC Level 1 (summarized above) and will vary depending on the type of security measures required to counter the specific nature of higher levels of threat. Such measures could include additional personnel or assigning additional responsibilities to current personnel for a limited period of time.

We did not consider capital improvements, such as building a fence, to be true MARSEC Levels 2 or 3 costs. The nature of the response to MARSEC Levels 2 and 3 is intended to be a quick surge of resources to counter an increased threat level. Capital improvements generally take time to plan and implement and could not be in place rapidly. Capital improvement costs are estimated under MARSEC Level 1 costs.

We did not calculate MARSEC Level 2 cost for the AMS rule because this will be primarily a cost to the Coast Guard for coordinating the heightened MARSEC Level in port and maritime areas.

To estimate a cost for MARSEC Level 2, we made assumptions about the length of time the nation's ports can be expected to operate at the heightened MARSEC Level. For the purpose of this assessment only, we estimate costs to the nation's ports elevating to MARSEC Level 2 twice a year, for 3 weeks each time, for a total period of 6 weeks at MARSEC Level 2. Again, this estimate of 6 weeks annually at MARSEC Level 2 is for the purposes of illustrating the order of magnitude of cost we can expect. Our estimate should not be interpreted as the Coast Guard's official position on how often the nation's ports will operate at MARSEC Level 2.

We estimated that there are Vessel Security Officers aboard all U.S. flag SOLAS vessels and most domestic vessels. We estimated that there will also be key crewmembers that can assist with security duties during MARSEC Level 2 aboard these vessels. We assumed that both Vessel Security Officers and key crewmembers will work 12 hours a day (8 hours of regular time, 4 hours of overtime) during the 42 days that the ports are at MARSEC Level 2. We then estimated daily and overtime rates for Vessel Security Officers and key crewmembers. Given these assumptions, we estimated that elevating the security level to MARSEC Level 2 twice a year each for 21 days will cost vessel owners and operators approximately \$235 million annually.

We estimated that every regulated facility will have a Facility Security Officer assigned to it. We also estimated that there will also be a key person that can assist with security duties during MARSEC Level 2 at each facility. We assumed that both Facility Security Officers and key personnel will work 12 hours a day (8 hours of regular time, 4 hours of overtime). For facilities that have to acquire security personnel for MARSEC Level 1, we assumed that during MARSEC Level 2 the number security guards would double for this limited time. For the facilities for which we did not assume any additional guards at MARSEC Level 1, we assumed that during MARSEC Level 2 these would have to acquire a minimal number of security guards. Given these assumptions, we estimated that elevating the security level to MARSEC Level 2 twice a year each for 21 days will cost facility owners and operators approximately \$424 million annually.

We estimated that elevating the security level to MARSEC Level 2 twice a year each for 21 days will cost the regulated OCS facility owners and operators approximately \$4 million annually. This cost is primarily due to increased cost for OCS Facility Security Officers and available key security personnel.

Other costs that we did not attempt to quantify include possible operational restrictions such as limiting cargo operations to daylight hours or greatly limiting access to facilities or vessels.

MARSEC Level 3 will involve significant restriction of maritime operations that could result in the temporary closure of individual facilities, ports, and waterways either in a region of the U.S. or the entire nation. Depending on the nature of the specific threat, this highest level of maritime security may have a considerable impact on the stakeholders in the affected ports or maritime areas. The ability to estimate the costs to business and government for even a short period at MARSEC Level 3 is virtually impossible with any level of accuracy or analytical confidence due to the infinite range of threats and scenarios that could trigger MARSEC Level 3.

The length and the duration of the increased security level to MARSEC Level 3 will be entirely dependent on the intelligence received and the scope of transportation security incidents or disasters that have already occurred or are imminent. While we can reasonably expect MARSEC Level 3 to increase the direct costs to businesses attributable to increased personnel or modified operations, we believe the indirect costs to society of the "ripple effects"

associated with sustained port closures would greatly outweigh the direct costs to individual businesses.

The U.S. Marine Transportation System (MTS)

The cost of MARSEC Level 3 can best be appreciated by the benefits of the MTS to the economy. Maritime commerce is the lifeblood of the modern U.S. trade-based economy, touching virtually every sector of our daily business and personal activities.

Annually, the MTS contributes significant benefits to the economy. More than 95 percent of all overseas trade that enters or exits this country moves by ship, including 9 million barrels of oil a day that heats homes and businesses and fuels our automobiles.¹ In addition, over \$738 billion of goods are transported annually through U.S. ports and waterways.²

Other benefits include the water transportation and the shipping industry that generate over \$24 billion in revenue and provides nearly \$3 billion of payrolls.³ The annual economic impact of cruise lines, passengers, and their suppliers is more than \$11.6 billion in revenue and 176,000 in jobs for the U.S. economy.⁴ Our national defense is also dependent on the MTS. Approximately 90 percent of all equipment and supplies for Desert Storm were shipped from strategic ports via our inland and coastal waterways.⁵

The Ripple Effect of Port Closures on the U.S. Economy

We could not only expect the immediate effects of port and waterway closures on waterborne commerce as described above, but also serious "ripple effects" for the entire U.S. economy that could last for months or more, including delayed commerce, decreased productivity, price increases, increased unemployment, unstable financial markets worldwide, and economic recession.

To appreciate the impact, we can examine just the agricultural sector of our economy. Many farm exports are just-in-time commodities, such as cotton shipped to Japan, South Korea, Indonesia, and Taiwan. Asian textile mills receive cotton on a just-in-time basis because these mills do not have warehousing capabilities. A port

shutdown may cause U.S. cotton wholesalers to lose markets, as textile producers find suppliers from other nations. U.S. wholesalers would lose sales until shipping is restored.

Another example is the auto industry. A recent shutdown of West Coast ports due to a labor dispute caused an automobile manufacturer to delay production because it was not receiving parts to make its cars. This demonstrates that a port shutdown can create a domino effect, from stalling the distribution of materials to causing stoppages and delays in production to triggering job losses, higher consumer prices, and limited selection.

The macroeconomic effects of the recent shutdown of West Coast ports, while not in response to a security threat, are a good example of the economic costs that we could experience when a threat would necessitate broad-based port closures. The cost estimates of this 11-day interruption in cargo flow and closure of 29 West Coast ports have ranged between \$140 million to \$2 billion a day, but are obviously high enough to cause significant losses to the U.S. economy.⁶

Another proxy for the estimated costs to society of nationwide port closures and the consequential impact on the U.S. supply chain can be seen by a recent war game played by businesses and government agencies.⁷ In that recent war game, a terrorist threat caused 2 major ports to close for 3 days, and then caused a nationwide port closure for an additional 9 days. This closure spanned only 12 days, but resulted in a delay of approximately 3 months to clear the resulting containerized cargo backlog. The economic costs of the closings attributable to manufacturing slowdowns and halts in production, lost sales, and spoilage was estimated at approximately \$58 billion. The simulation gauged how participants would respond to an attack and the ensuing economic consequences. Furthermore, a well-coordinated direct attack of multiple U.S. ports could

shutdown the world economy by effectively halting international trade flows to and from the U.S. market—the largest market for goods and services in the world.

We believe that the cost to the national economy of a port shutdown due to extreme security threats, while not insignificant, would be relatively small if it only persisted for a few days and involved very few ports. However, if the interruption in cargo flows would persist much longer than the 11-day shutdown recently experienced on the West Coast, the economic loss is estimated to geometrically increase (double) every additional 10 days the ports were closed.⁸ At a certain point, companies would start declaring bankruptcies, people would be laid off indefinitely, and the prices of goods would increase. This effect would continue and intensify until alternate economic activities took place, such as the unemployed finding less desirable jobs or companies finding secondary lines of operations and suppliers. Regardless, the economic hardship suffered by industry, labor, and the loss of public welfare due to a sustained nationwide port shutdown may have as significant an effect on the U.S. as the act of terror itself.

Benefit Assessment

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

⁶ See *Lost Earnings Due to West Coast Port Shutdown—Preliminary Estimate*, Patrick Anderson, October 7, 2002, available at <http://www.AndersonEconomicGroup.com>; An Assessment of the Impact of West Coast Container Operations and the Potential Impacts of an Interruption of Port Operations, 2000, Martin Associates, October 23, 2001, available from the Pacific Maritime Association. These two studies were widely quoted by most U.S. news services including Sam Zuckerman, San Francisco Chronicle, October 2002.

⁷ The war game simulation was designed and sponsored by Booz Allen Hamilton and The Conference Board, details available at <http://www.boozallen.com/>.

⁸ See Anderson.

¹ See MTS Fact Sheet available at www.dot.gov/mts/fact_sheet.htm.

² See 2000 Exports and Imports by U.S. Customs District and Port available at www.marad.dot.gov/statistics/usfwt/.

³ U.S. Census Bureau, 1997 Economic Census, Transportation and Warehousing-Subject Series.

⁴ See footnote 1.

⁵ See footnote 1.

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. Table 1 presents the annual risk points reduced by the final rules. As shown, the final rule for vessel

security reduces the most risk points annually. The final rule for AIS reduces the least.

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

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

Once we determined the annual risk points reduced, we discounted these estimates to their present value (7 percent discount rate, 2003–2012) so that they could be compared to the costs. We presented the cost

effectiveness, or dollars per risk point reduced, in two ways: First, we compared first-year cost to 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 to 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 plans	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.

As shown, the final rule for vessel security is the most cost effective. This is due to the nature of the security measures we expect vessels will have to take to ensure compliance as well as the level of risk that is reduced by those measures. Facility security is less cost effective because facilities incur higher costs for capital purchases (such as gates and fences) and require more labor (such as security guards) to ensure security. OCS Facility and AMS Plans are almost equally cost effective; the entities these final rules cover do not incur the highest expenses for capital equipment, but on this relative scale, they do not receive higher risk reduction in the N-RAT, either. The AIS final rule is the least cost effective, though it is important to remember that AIS provides increased maritime domain awareness and navigation safety, which is not robustly captured using the N-RAT.

Small Entities

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

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

Analysis” for these final rules in each of their respective dockets, where indicated under **ADDRESSES**.

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

Assistance for Small Entities

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

We have placed Small Business Compliance Guides in the dockets for the Area Maritime, Vessel, and Facility Security and the AIS rules. These

Compliance Guides will explain the applicability of the regulations, as well as the actions small businesses will be required to take in order to comply with each respective final rule. We have not created Compliance Guides for this final rule (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].

Comments regarding collection of information are addressed in the "Discussion of Comments and Changes" sections of each final rule. You are not required to respond to a collection of information unless it displays a currently valid OMB control number. We received OMB approval for these collections of information on June 16, 2003. They are valid until December 31, 2003.

Federalism

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

authority conflicts with the exercise of Federal authority under the Federal statute.

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

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

Finally, it is important to note that the regulations implemented by this final

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

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

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

As stated in the temporary interim rule for part 101 (68 FR 39277), we believe that the federalism principles enumerated by the Supreme Court in *U.S. v. Locke*, 529 U.S. 89 (2000), regarding field preemption of certain State vessel safety, equipment, and operating requirements extends equally to this final rule, especially regarding the longstanding history of significant Coast Guard maritime security regulations and control of vessels for security purposes. It would be inconsistent with the federalism principles stated in Executive Order 13132 to construe the MTSA as not preempting State regulations that conflict with these regulations. Vessels and shipping companies, particularly, would be confronted with an unreasonable burden if they had to comply with varying requirements as they move from state to state.

Ten commenters addressed the disclosure of security plan information. One commenter advocated making security plans public. One commenter was concerned that plans will be disclosed under 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 some State laws require full disclosure of public documents. Three commenters supported our conclusion that the MTSA and our regulations preempt any conflicting State requirements. Another commenter was particularly pleased to observe the strong position taken by the Coast Guard in support of Federal preemption of conflicting 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.

One commenter stated that there is a "real cost" to implementing security measures, and it is significant. The commenter stated that there is a disparity between Federal funding dedicated to air transportation and

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

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

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

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

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

We are using the same cooperative arrangement that we have used with success in the safety realm by accepting SOLAS certificates documenting flag-state approval of foreign SOLAS Vessel Security Plans that comply with the comprehensive requirements of the ISPS Code. The consistency of the international and domestic security

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

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

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

Unfunded Mandates Reform Act

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

the regulatory action as required by the Act because it is necessary for the national security of the United States (2 U.S.C. 1503(5)). We did not receive comments regarding the Unfunded Mandates Reform Act.

Taking of Private Property

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

Civil Justice Reform

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

Protection of Children

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

Indian Tribal Governments

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

Energy Effects

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

not designated it as a significant energy action. Therefore, it does not require a Statement of Energy Effects under Executive Order 13211.

This final rule has a positive effect on the supply, distribution, and use of energy. The final rule provides for security assessments, plans, procedures, and standards, which will prove beneficial for the supply, distribution, and use of energy at increased MARSEC Levels. We did not receive comments regarding energy effects.

Environment

We have considered the environmental impact of this final rule and concluded that, under Commandant Instruction M16475.ID, there are no factors in this case that would limit the use of a categorical exclusion under section 2.B.2 of the Instruction. Therefore, this final rule is categorically excluded, under figure 2-1, paragraphs (34)(a), (34)(c), (34)(d), and (34)(e) of the Instruction from further environmental documentation.

This final rule concerns security assessments, plans, training, positions, and organizations along with vessel equipment requirements 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 rule will be done in conjunction with appropriate State coastal authorities. The Coast Guard will, therefore, comply with the requirements of the Coastal Zone Management Act while furthering its intent to protect the coastal zone. We did not receive comments regarding the environment.

List of Subjects

33 CFR Part 2

Administrative practice and procedure, Law enforcement.

33 CFR Part 101

Facilities, Harbors, Maritime security, Ports, Security assessments, Security plans, Reporting and recordkeeping requirements, Vessels, Waterways.

33 CFR Part 102

Maritime security.

■ Accordingly, the Coast Guard amends 33 CFR part 2 as follows and the interim rule adding 33 CFR parts 101 and 102 that was published at 68 FR 39240 on July 1, 2003, and amended at 68 FR 41914 on July 16, 2003, is adopted as a final rule with the following changes:

PART 2—JURISDICTION

- 1. Revise the authority citation for part 2 to read as follows:

Authority: 14 U.S.C. 633; 33 U.S.C. 1222; Pub. L. 89-670, 80 Stat. 931, 49 U.S.C. 108; Pub. L. 107-296, 116 Stat. 2135, 2249, 6 U.S.C. 101 note and 468; Department of Homeland Security Delegation No. 0170.1.

§ 2.22 [Amended]

- 2. In § 2.22(a)(1)(i), after the words "within subtitle II", add the words "and subtitle VI".

PART 101—MARITIME SECURITY: GENERAL

- 3. The authority citation for part 101 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191, 192; Executive Order 12656, 3 CFR 1988 Comp., p. 585; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

- 4. Revise the heading to part 101 to read as shown above.
- 5. In § 101.100, in the introductory text of paragraph (a), remove the word "part" and add, in its place, the word "subchapter", and add new paragraph (c) to read as follows:

§ 101.100 Purpose.

* * * * *

(c) The assessments and plans required by this subchapter are intended for use in implementing security measures at various MARSEC Levels. The specific security measures and their implementation are planning criteria based on a set of assumptions made during the development of the security assessment and plan. These assumptions may not exist during an actual transportation security incident.

- 6. In § 101.105—
 - a. In the definition of "Barge fleeting facility", remove the word "permitted" and add, in its place, the words "subject to permitting", and, after the words "33 CFR part 322", add the words ", part 330, or pursuant to a regional general permit";
 - b. In the definition of "Cargo", at the end of the paragraph, add the words ", except dredge spoils";
 - c. In the definition of "Certain Dangerous Cargo (CDC)", remove the text "33 CFR 160.203" and add, in its place, the text "33 CFR 160.204";
 - d. In the definition of "Company Security Officer (CSO)", remove the text "OSC" wherever it appears, and add, in its place, the text "OCS" and remove the word "COTP" and add, in its place, the words "Coast Guard";
 - e. In the definition for "Declaration of Security (DoS)", remove the word

“interface” wherever it appears and add, in its place, the word “activity”;

■ f. In the definition for “Passenger vessel”, paragraph (1), after the word “passengers” add the words “, including at least one passenger-for-hire”;

■ g. In the definitions for “Vessel-to-facility interface”, “Vessel-to-port interface”, and “Vessel-to-vessel activity” remove the word “goods” wherever it appears and add, in its place, the words “cargo, vessel stores,”;

■ h. Revise the definitions for “Dangerous substances or devices”, “International voyage”, “Owner or operator”, “Unaccompanied baggage”, and “Waters subject to the jurisdiction of the U.S.” to read as set out below; and

■ i. Add, in alphabetical order, definitions for “Breach of security”, “Cargo vessel”, “Dangerous goods and/or hazardous substances”, “General shipyard facility”, and “Public access facility” to read as follows:

§ 101.105 Definitions.

* * * * *

Breach of security means an incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.

* * * * *

Cargo vessel means a vessel that carries, or intends to carry, cargo as defined in this section.

* * * * *

Dangerous goods and/or hazardous substances, for the purposes of this subchapter, means cargoes regulated by parts 126, 127, or 154 of this chapter.

Dangerous substances or devices means any material, substance, or item that reasonably has the potential to cause a transportation security incident.

* * * * *

General shipyard facility means—

(1) For operations on land, any structure or appurtenance thereto designed for the construction, repair, rehabilitation, refurbishment, or rebuilding of any vessel, including graving docks, building ways, ship lifts, wharves, and pier cranes; the land necessary for any structures or appurtenances; and the equipment necessary for the performance of any function referred to in this definition; and

(2) For operations other than on land, any vessel, floating drydock, or barge used for, or a type that is usually used for, activities referred to in paragraph (1) of this definition.

* * * * *

International voyage means a voyage between a country to which SOLAS applies and a port outside that country.

A country, as used in this definition, includes every territory for the internal relations of which a contracting government to the convention is responsible or for which the United Nations is the administering authority. For the U.S., the term “territory” includes the Commonwealth of Puerto Rico, all possessions of the United States, and all lands held by the U.S. under a protectorate or mandate. For the purposes of this subchapter, vessels solely navigating the Great Lakes and the St. Lawrence River as far east as a straight line drawn from Cap des Rosiers to West Point, Anticosti Island and, on the north side of Anticosti Island, the 63rd meridian, are considered on an “international voyage” when on a voyage between a U.S. port and a Canadian port.

* * * * *

Owner or operator means any person or entity that owns, or maintains operational control over, any facility, vessel, or OCS facility subject to this subchapter. This includes a towing vessel that has operational control of an unmanned vessel when the unmanned vessel is attached to the towing vessel and a facility that has operational control of an unmanned vessel when the unmanned vessel is not attached to a towing vessel and is moored to the facility; attachment begins with the securing of the first mooring line and ends with the casting-off of the last mooring line.

* * * * *

Public access facility means a facility—

- (1) That is used by the public primarily for purposes such as recreation, entertainment, retail, or tourism, and not for receiving vessels subject to part 104;
- (2) That has minimal infrastructure for servicing vessels subject to part 104 of this chapter; and
- (3) That receives only:
 - (i) Vessels not subject to part 104 of this chapter, or
 - (ii) Passenger vessels, except:
 - (A) Ferries certificated to carry vehicles;
 - (B) Cruise ships; or
 - (C) Passenger vessels subject to SOLAS Chapter XI.

* * * * *

Unaccompanied baggage means any baggage, including personal effects, that is not being brought on board on behalf of a person who is boarding the vessel.

* * * * *

Waters subject to the jurisdiction of the U.S., for purposes of this subchapter, includes all waters described in section 2.36(a) of this

chapter; the Exclusive Economic Zone, in respect to the living and non-living resources therein; and, in respect to facilities located on the Outer Continental Shelf of the U.S., the waters superjacent thereto.

■ 7. In § 101.120—

■ a. In paragraph (b)(1), remove the words “engage on international voyages and facilities that serve only vessels on international voyages” and add, in their place, the words “are subject to SOLAS Chapter XI”;

■ b. In paragraph (b)(3), add the following words to the end of the last sentence: “and a vessel, facility, or Outer Continental Shelf facility specific security assessment report generated under the Alternative Security Program”;

■ c. Add paragraph (b)(4) to read as set out below;

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

■ e. Add paragraphs (e) and (f) to read as follows:

§ 101.120 Alternatives.

* * * * *

(b) * * *

(4) Owners or operators shall make available to the Coast Guard, upon request, any information related to implementation of an approved Alternative Security Program.

* * * * *

(d) *Amendment of Approved Alternative Security Programs.* (1) Amendments to an Alternative Security Program approved under this section may be initiated by—

(i) The submitter of an Alternative Security Program under paragraph (c) of this section; or

(ii) The Coast Guard upon a determination that an amendment is needed to maintain the security of a vessel or facility. The Coast Guard will give the submitter of an Alternative Security Program written notice and request that the submitter propose amendments addressing any matters specified in the notice. The submitter will have at least 60 days to submit its proposed amendments.

(2) Proposed amendments must be sent to the Commandant (G-MP). If initiated by the submitter, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the Commandant (G-MP) allows a shorter period. The Commandant (G-MP) will approve or disapprove the proposed amendment in accordance with paragraph (f) of this section.

(e) *Validity of Alternative Security Program.* An Alternative Security

Program approved under this section is valid for 5 years from the date of its approval.

- (f) The Commandant (G-MP) will examine each submission for compliance with this part, and either:
 - (1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;
 - (2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or
 - (3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

■ 8. Add the text to § 101.125 to read as follows:

§ 101.125 Approved Alternative Security Programs.

The following have been approved, by the Commandant (G-MP), as Alternative Security Programs, which may be used by vessel or facility owners or operators to meet the provisions of parts 104, 105, or 106 of this subchapter, as applicable:

- (a) American Gaming Association Alternative Security Program, dated September 11, 2003.
- (b) American Waterways Operators Alternative Security Program for Tugboats, and Towboats and Barges, dated September 24, 2003.
- (c) Passenger Vessel Association Industry Standards for Security of Passenger Vessels and Small Passenger Vessels, dated September 17, 2003.

§ 101.205 [Amended]

■ 9. In § 101.205, in table 101.205, remove the words “Elevated: Blue” and “Guarded: Yellow.”, and add, in their place, the words “Guarded: Blue” and “Elevated: Yellow” respectively.

§ 101.300 [Amended]

- 10. In § 101.300—
 - a. In paragraph (a), remove the words “a Maritime Security Directive issued under section 101.405 of this part” and add, in their place, the words “an electronic means, if available”; and
 - b. In paragraphs (c)(1) and (c)(2), remove the word “confirm” and add, in its place, the words “ensure confirmation”.

§ 101.405 [Amended]

■ 11. In § 101.405(a)(2), remove the words “require the owner or operator to prove that they have a ‘need to know’ the information in the MARSEC Directive and that they are a ‘covered person,’ as those terms are defined in 49 CFR part 1520” and add, in their place, the words “require owners or operators to prove that they are a person required by 49 CFR 1520.5(a) to restrict disclosure of and

access to sensitive security information, and that under 49 CFR 1520.5(b), they have a need to know sensitive security information”.

§ 101.410 [Amended]

- 12. In § 101.410(b)(8), remove the words “For U.S. vessels, suspension or revocation of security plan approval”, and add, in their place, the words “Suspension or revocation of a security plan approved by the U.S.”.
- 13. In § 101.420, revise paragraph (b) to read as follows:

§ 101.420 Right to appeal.

* * * * *

(b) Any person directly affected by a decision or action taken by a District Commander, whether made under this subchapter generally or pursuant to paragraph (a) of this section, with the exception of those decisions made under § 101.410 of this subpart, may appeal that decision or action to the Commandant (G-MP), according to the procedures in 46 CFR 1.03-15. Appeals of District Commander decisions or actions made under § 101.410 of this subpart should be made to the Commandant (G-MOC), according to the procedures in 46 CFR 1.03-15.

* * * * *

■ 14. In § 101.505(b), at the end of the paragraph, add a sentence to read as follows:

§ 101.505 Declaration of Security (DoS).

* * * * *

(b) * * * A DoS must, at a minimum, include the information found in the ISPS Code, part B, appendix 1 (Incorporated by reference, see § 101.115).

* * * * *

§ 101.510 [Amended]

- 15. In § 101.510, in the introductory text—
 - a. Remove the word “risk” and add, in its place, the word “security”; and
 - b. After the words “These tools”, add the word “may”.
- 16. In § 101.515 add paragraph (c) to read as follows:

§ 101.515 Personal identification.

* * * * *

(c) Vessel, facility, and OCS facility owners and operators must permit law enforcement officials, in the performance of their official duties, who present proper identification in accordance with this section to enter or board that vessel, facility, or OCS facility at any time, without delay or obstruction. Law enforcement officials, upon entering or boarding a vessel,

facility, or OCS facility, will, as soon as practicable, explain their mission to the Master, owner, or operator, or their designated agent.

PART 102—MARITIME SECURITY: NATIONAL MARITIME TRANSPORTATION SECURITY [RESERVED]

■ 17. Revise the heading to part 102 to read as shown above.

Dated: October 8, 2003.
Thomas H. Collins,
Admiral, Coast Guard, Commandant.
 [FR Doc. 03-26345 Filed 10-20-03; 8:45 am]
BILLING CODE 4910-15-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 103
[USCG-2003-14733]
RIN 1625-AA42

Area Maritime 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 establishes U.S. Coast Guard Captains of the Ports as Federal Maritime Security Coordinators, and establishes requirements for Area Maritime Security Plans and Area Maritime Security Committees. This rule is one in a series of final rules on maritime security published in today’s **Federal Register**. To best understand this final 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-2003-14733 and are available for inspection or copying at the Docket Management Facility, U.S. Department of Transportation, room PL-401, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this

docket on the Internet at <http://dms.dot.gov>.

FOR FURTHER INFORMATION CONTACT: If you have questions on this final rule, call Lieutenant Commander Richard Teubner (G-MPS-2), U.S. Coast Guard by telephone 202-267-4129 or by electronic mail

rteubner@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 "Area Maritime Security" in the **Federal Register** (68 FR 39284). 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 41914).

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

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

In order to focus on the changes made to the regulatory text since the

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

Background and Purpose

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

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 concerns applicability and applies the requirements for Area Maritime Security to all vessels and facilities located in, on, under, or adjacent to waters subject to the jurisdiction of the U.S.

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.

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 chapter I, 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 Maritime Security (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 a specific security concern.

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." 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 AMS Plans.

We received comments from the Environmental Protection Agency regarding the effects of our regulations on EPA-regulated oil facilities. These comments focused primarily on the potential overlapping provisions of 33 CFR part 105 and 40 CFR part 112. Overlap exists in four major areas: Notification of security incidents, fencing and monitoring, evacuation procedures, and security assessments. In cases of overlapping provisions for oil facilities regulated both in parts 105 and 112, the requirements in our final rules and EPA rulemakings do not supplant one another. Additionally, an EPA-regulated facility need not amend the facility's Spill Prevention Control and Countermeasure Plan or Facility Response Plan, as we first stated in the temporary interim rule (68 FR 39251) (part 101). We will be working further with EPA in the implementation of these final rules to minimize the burden to the facilities while ensuring that these facilities are secure. It is our belief that response plans for EPA-regulated oil facilities will serve as an excellent foundation for security plans that may be required under our regulations.

EPA asked for clarification for facilities adjacent to the navigable waters that handle or store cargo that is hazardous or a pollutant but may not be marine transportation related facilities. These facilities are covered by parts 101 through 103 of subchapter H 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. The AMS Assessment may reveal that these EPA-regulated facilities may be involved in a transportation security incident and the COTP may direct these facilities, through orders issued under existing COTP authority, to implement security measures based on the facilities' operations and the MARSEC Level. We encourage owners and operators of these EPA-regulated facilities, as well as representatives from EPA, to participate in AMS Committee activities.

EPA asked for further clarification on drills and exercises requirements. As we stated in the temporary interim rule, non-security drills and exercises may be combined with security drills to minimize burden. Additionally, EPA-regulated facilities that conduct drills not related to security are encouraged to

communicate with the local COTP and coordinate their drills at the area level. It is our intention to give facilities and vessels in the port area as much notice as practicable prior to an AMS Plan exercise to reduce the burden to those entities. Again, we encourage owners and operators of these EPA-regulated facilities, and EPA, to participate in AMS Committee activities to maximize coordination and minimize burden.

EPA asked us to clarify the role of Area Contingency Plans with the requirements of our final rules. Our rules are intended to work in concert with Area Contingency Plans and do not preempt their requirements. We envision that many members of the Area Committees who are responsible for implementing Area Contingency Plans will also become members of the AMS Committee. This participation will help ensure that implementing an AMS Plan will not conflict with an Area Contingency Plan.

Finally, EPA asked for clarification on requirements for marine transportation related facilities that handle petroleum oil, non-petroleum oil, and edible oil. These facilities are directly regulated under § 105.105(a)(1) and must meet the requirements of part 105.

Subpart B—Federal Maritime Security Coordinator (FMSC)

This subpart designates the Coast Guard COTP as the Federal Maritime Security Coordinator and provides a description of the COTP's authority as Federal Maritime Security Coordinator to establish, convene, and direct the AMS Committee.

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 International Ship and Port Facility Security (ISPS) Code, part A, section 16.5, by using the AMS Plan to satisfy our international obligations to communicate to IMO, as required by the International Convention for Safety of Life at Sea, 1974 (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.

Subpart C—Area Maritime Security (AMS) Committee

This subpart describes the composition and responsibilities of the AMS Committee.

One commenter supported the creation of AMS Committees, stating that through the partnership between industry and the Coast Guard, the committees will develop a comprehensive plan for the security of the port.

Two commenters supported the creation of AMS Committees if they were composed of appropriately experienced representatives from a variety of sources in the port. One commenter stated that the AMS Committee allows for "port specific" appropriate risk mitigation as opposed to a blanket risk mitigation policy placed on the entire U.S. waterway system and will strengthen the AMS Plan with the "buy in" of the maritime community.

We agree with the commenters and believe that the AMS Committee is a vital link to ensuring the port community is involved in security and its implementation. The inclusive nature of the AMS Committee and the active involvement of a variety of port stakeholders, bringing their experience within the maritime community to the table, will enhance the success of the AMS Committee in drafting the AMS Plan.

One commenter stated that the AMS Committee should have the responsibility to identify Federal, State, Indian Tribal, and local government agencies and law enforcement entities with jurisdiction over port-related matters.

We believe the responsibilities of Federal, State, Indian Tribal, and local government agencies and law enforcement entities with jurisdiction over port security related matters should be addressed in the AMS Plan and, therefore, have amended § 103.505.

Six commenters requested that the Coast Guard establish, without delay, an AMS Committee for the Outer Continental Shelf (OCS) portion of the Gulf of Mexico as an essential step in moving the various Federal law enforcement agencies and industry toward a mutual understanding of the response to a transportation security incident on the Outer Continental Shelf.

We intend to cover OCS facilities in the Gulf of Mexico by a single, District-

wide plan. The establishment of an AMS Committee for the OCS facilities in the Gulf of Mexico was discussed at recent Gulf Safety Committee and National Offshore Safety Advisory Committee (NOSAC) meetings. We intend to form an AMS Committee for this area in the near future. Additionally, owners and operators of OCS facilities are encouraged to participate on the AMS Committee of the COTP zone that is most relevant to their operations.

We received nine comments dealing with the protection of information shared with the AMS Committee. One commenter recommended that threat and risk assessments be kept at the government level so that this type of information would not be available to the public. Five commenters suggested that security plans or proprietary information regarding facilities or vessels be classified as confidential and not be shared with the AMS Committee. Four commenters requested that uniform guidance be provided to the AMS Committee on the handling of sensitive security information.

Section 103.300 provides that each AMS Committee will operate under a written charter that, among other items, details the rules for handling and protecting classified, sensitive security, commercially sensitive, and proprietary information. Threat and risk assessments developed by the AMS Committee will be embodied in written reports that will be designated sensitive security information and hence will not be available to the public.

Three commenters stated that the regulations do not indicate that the AMS Committee will function in a manner consistent with the procedures of Navigation and Vessel Inspection Circular (NVIC) 09-02, Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports. Two commenters stated that the regulations did not specify the identity of the "chartering entity" for the AMS Committee.

Section 101.105 states that the port security committee established under NVIC 09-02 may be the AMS Committee. The requirements for AMS Committees described in part 103 are consistent with NVIC 09-02. Therefore, AMS Committees will function in a manner consistent with the procedures of NVIC 09-02, unless the Committee agrees in its charter to a different arrangement. The AMS Committee is chartered under the direction of the COTP.

We received nine comments on AMS Committee participation. Three commenters urged the Coast Guard to

include the recreational boating community in all decisions that could limit recreational boaters' access to the water, stating that the future health of the community depends on reasonable access to the nation's waterways. Two commenters requested that private industry facility operators be allowed to fully participate in the AMS Committee. One commenter requested that utility representatives be allowed to fully participate in the AMS Committee. One commenter requested that government agencies that have roles in maritime and cargo security be involved in the AMS Committee. One commenter requested that representatives from the charterboat industry be included as AMS Committee members.

We encourage members of all affected communities, including small businesses, utilities, government officials, charterboats, and recreational boating, to become involved in maritime security through their local AMS Committees. Where appropriate, AMS Committees should include representatives from associations that represent all of these communities. Additionally, to ensure consistency across modes of transportation and with other Federal security programs, the Coast Guard intends to invite officials nominated by other Federal agencies, including the Transportation Security Administration (TSA), the Bureau of Customs and Border Protection and the Maritime Administration to participate in, and to appoint them as members of, the AMS Committees.

Eight commenters suggested that the criteria for AMS Committee membership or participation in a leadership position be revised. Currently, § 103.305(a) requires "at least 5 years of experience related to maritime or port security operations." Four commenters suggested that membership not be limited only to security-related experience. One commenter recommended that the seven AMS Committee members "must be selected from" the seven areas listed in § 103.305.

We aligned § 103.305 with the requirements for the AMS Committee found in the Maritime Transportation Security Act of 2002 (MTSA), which specifically requires a minimum of 7 members with at least 5 years of practical experience in maritime security operations and provides that the members "may be selected" from the seven areas listed. We have, however, amended § 103.305 in order to clarify that, while 7 members of the AMS Committee must have at least 5 years of experience related to maritime or port security operations, the AMS

Committee may be composed of more than 7 members. We are also adding labor to the list of areas from which AMS Committee members should be selected. These changes increase participation in the AMS Committee, which we believe will be beneficial to the operation of the AMS Committee.

One commenter recommended that AMS Committees consider information access "up the chain of command" for "strong and viable seaport security."

The COTP is the Federal Maritime Security Coordinator, and will be involved with the AMS Committee. The COTP is responsible for disseminating information to the port stakeholders and "up the chain of command." Additionally, owners or operators of vessels and facilities subject to parts 104, 105, and 106 are required to report all suspicious activities and breaches of security to the National Response Center (NRC); other owners and operators are encouraged to do so. Finally, non-compliance with security plans and the reporting requirements in them must be reported to the Coast Guard.

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

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

One commenter stated that, because vessel and facility owners or operators may be required under Federal law to obtain the services of security guards and armed guards, there should be minimum standards guiding the qualifications, certification, and performance of those guards. The commenter also suggested that the AMS Committee evaluate local armed security service providers and develop a list of qualified providers.

As we stated in the temporary interim rule (68 FR 39255) (part 101), we intend to work with State homeland security representatives to encourage the review of all standards related to armed personnel. While we have not required each AMS Committee to develop lists of qualified security personnel providers, each AMS Committee may undertake this task.

Subpart D—Area Maritime Security (AMS) Assessment

This subpart directs the AMS Committee to ensure development of a risk-based AMS Assessment.

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 using the penalties provision under § 101.415.

One commenter stated that any third party participating in developing the AMS Assessment should sign non-disclosure or secrecy agreements regarding any classified, sensitive security, commercially sensitive, or proprietary information developed, collected, or otherwise accessed during the preparation of the AMS Assessment.

If the AMS Committee or the Coast Guard chooses to use third parties in developing the AMS Assessment or the AMS Plan, those third parties must possess the same level of clearance as the material they are helping to develop, collect, or otherwise access. As required by § 103.300(b)(6), the charter under which the AMS Committee operates will establish rules for handling and protecting classified and sensitive security information. We intend to address third parties signing non-disclosure or secrecy agreements to

protect classified or sensitive security information in future guidance.

One commenter supported the development of a risk-based AMS Assessment but requested the addition of assessment requirements to specifically include: (1) Consideration of requiring Facility Security Plans and Vessel Security Plans for vessels that carry fewer than 150 passengers or facilities that serve these smaller operators, and (2) consideration of the public transit sector. The commenter stated that adding requirements to assess smaller operations would address a gap created because the current regulations exempt vessels and facilities that handle 150 passengers or fewer. Furthermore, the commenter stated that a critical look at the public transit sector (*e.g.*, ferry vessels) was needed because implementing certain security measures could severely hurt this industry and could cause a security inequity with other public transportation modes. The commenter further suggested that the public transit sector should be allowed to come forward with security recommendations to satisfy the AMS Plan.

We agree that both the consideration of small vessel and facility operations as well as public transit must be included in the AMS Assessment. Section 103.405 was developed to cover these topics but did not go into detail. We believe the details of the AMS Assessment are best embodied in guidance. We intend to provide additional guidance in a revision to NVIC 9–02 (Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports). We intend to update this guidance to incorporate several suggestions and address the consideration of security measures for vessels and facilities that are not directly regulated under parts 104 or 105 but, due to the specific nature of their port location or operation, may require additional security measures or requirements. Public transit issues and parity with other transportation modes is also a concern. The AMS Assessment is required to address transportation infrastructure, which includes all ferry operations, as well as train or other modes affecting the area maritime community.

One commenter stated that the AMS Assessment should include consideration of manufacturers and users of hazardous material.

Section 103.405 lists the elements that must be taken into consideration in developing the AMS Assessment. These elements are broadly defined and could include manufacturers and users of hazardous materials if they may be

involved in a transportation security incident.

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 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, potential conflicts between security plans and the AMS Plan will be identified during the Facility Security Plan approval process.

Subpart E—Area Maritime Security (AMS) Plan

This subpart concerns the elements of the AMS Plan, requirements on exercising the AMS Plan, and recordkeeping requirements.

One commenter supported the creation of an AMS Plan and believes it provides details of operational and physical measures that must be in place at all MARSEC Levels rather than blanket security rules that do not appropriately apply to the public transit sector (*e.g.*, ferry vessels).

We believe the AMS Plan is an excellent tool to coordinate and communicate security measures throughout the port community. The AMS Plan takes into account unique port operations and their criticality to the community and tailors security measures to effectively continue essential port operations as MARSEC Levels increase.

One commenter asked that we ensure the interoperability of the various plans required in parts 101 through 106, stating that we must have a coordinated approach to the implementation of national maritime security requirements.

We agree with the commenter and intend to take the interoperability of security plans into account as we review and approve security plans for vessels

and facilities and as we develop the National and AMS Plans.

One commenter stated that there should be a common template for AMS Plans for use at all Districts.

The regulations provide uniformity by requiring all AMS Plans to be submitted for review to the Coast Guard District Commander and for approval to the Coast Guard Area Commander.

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 "vital 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, the Vessel Security Plan 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.

Two commenters asked if the COTP would allow private port facilities access to the completed AMS Assessment or Plan, stating that a port plan could potentially contradict a private Facility Security Plan. One commenter stated that the AMS Plan should be "absolutely unequivocal about the lines of authority for preventative and response actions as well as law enforcement."

The development of the AMS Plan is a collaborative effort between Federal, State, Indian Tribal, and local agencies as well as individual facility owners and any other interested stakeholders. AMS Plans contain sensitive security information, and the COTP must ensure it is protected in accordance with 49 CFR part 1520. The Coast Guard will resolve potential conflicts between an individual Facility Security Plan and the AMS Plan during the Facility Security Plan approval process, which will ensure proper planning for preventative and response actions. To clarify that the entire AMS Plan is not necessarily sensitive security information, we are amending § 103.500(b) to allow only those portions of the AMS Plan that contain sensitive security information to be marked as such. This will allow certain non-sensitive security information portions of the AMS Plan to be widely distributed to maximize its communication and coordination with port stakeholders.

Ten commenters addressed the disclosure of security plan information. One commenter advocated 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 some State laws require full disclosure of public documents. Three commenters supported our conclusion that the MTSA and our regulations preempt any conflicting State requirements. Another commenter was particularly pleased to observe the strong position taken by the Coast Guard in support of Federal preemption of conflicting 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.

Four commenters urged us to conduct background checks on potential members of AMS Committees because the information contained in the AMS Plans might be “secret.” Two commenters urged us to designate security assessments, Vessel Security Plans, Facility Security Plans, and information contained in the AMS Plans as “secret,” and require secret clearance for AMS Committee members.

We do not believe that a security designation above sensitive security information is needed for this material. However, § 103.300(b)(6) requires AMS Committee charters to include rules for handling and processing classified material. Access to the AMS Plan will be limited to those on the AMS Committee who have agreed to protect the material in a manner appropriate to its security sensitivity and have a need to know the material. Guidance on sensitive security information and its use will be issued to assist AMS Committee members, consistent with 49 CFR part 1520. For material that is designated at a level higher than sensitive security information, the Coast Guard will screen AMS Committee members for appropriate clearances and take precautions appropriate to the material’s sensitivity. Individuals and Federal, State, Indian Tribal, and local agencies outside those with transportation oversight authority will not be allowed to view plans or assessments of vessels and facilities unless circumstances provide a need to view them. As stated in the “Vessel Security” temporary interim rule (68 FR 39297), certain portions of each Vessel Security Plan and Vessel Security Assessment must be made accessible to authorities; however, those portions not required to be disclosed are protected with the sensitive security information designation and need-to-know criteria. Owners and operators of vessels and

facilities may also request a determination of a higher designation than sensitive security information for their plans. The Commandant or the COTP, whoever is responsible for reviewing the security plan, will retain the designation authority. In all cases, the material, if retained by a Federal agency, must be safeguarded to the appropriate designation.

We received 28 comments regarding communication of changes in the MARSEC Levels. Most commenters were concerned about the Coast Guard’s capability to communicate timely changes in MARSEC Levels to facilities and vessels. Some stressed the importance of MARSEC Level information reaching each port area in the COTP’s zone and the entire maritime industry. Some stated that local Broadcast Notice to Mariners and MARSEC Directives are flawed methods of communication and stated that the only acceptable 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 or facility owners and 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.

We received four comments on the subject of AMS Plan exercises. One commenter agreed with our inclusion of tabletop exercises as a cost-effective means of exercising the security plan. Two commenters supported a maritime security field training exercise in each area covered by an AMS Plan but requested that the frequency be every 3 years rather than annually. These commenters stated that the annual requirement for an AMS Plan exercise placed an undue burden on the maritime sector because it is already conducting vessel and facility exercises. One commenter stated that the Coast Guard must be aware that the AMS exercise requirements may be overly burdensome to some vessels, as they

could potentially be required to participate in several AMS exercises per year.

We believe that exercising the AMS Plan annually is essential to ensure that it can be effectively implemented, stakeholders with security responsibilities are proficient in their responsibilities, and any deficiencies in the AMS Plan can be identified and corrected in a timely manner. In addition, the AMS Plan exercise frequency must also meet the international requirement for an annual exercise found in the ISPS Code, part B, regulation 18.6. However, we realize that an AMS Plan annual exercise requirement is in addition to the annual exercise requirements for Vessel and Facility Security Plans. We also recognize that many of the entities affected by § 103.515 are also subject to, or regularly participate in, other emergency response or crisis management exercises. We are mindful of the potential burdens imposed on the regulated community, and other port stakeholders by the number of safety, security and response exercises required by various regulations, and believe that the objectives for AMS Plan exercises can often be met through effective consolidation of exercises. Further, we acknowledge that several vessels may be offered the opportunity to participate in several AMS Plan exercises per year. Participation in these AMS Plan exercises will be subject to the specific details of the AMS Plan as developed by the AMS Committee on which those vessel owners or operators may participate. While vessel owners and operators will be encouraged to participate in AMS Plan exercises and may be requested to deviate from normal operations to minimize interference with the AMS Plan exercise, they will not be required to participate. In addition, we anticipate that COTPs will give ample notice of AMS Plan exercises to allow vessel owners and operators to plan appropriately and to minimize the impact on the maritime community.

Section 103.515(c) allows the cognizant District Commander to authorize AMS Plan exercise credit for actual increases in the MARSEC Level and implementation of security measures during periods of critical port operations or special marine events. However, upon further review, we have decided to revise § 103.515(c) to provide an additional option to participate in another port exercise that contains elements of the AMS Plan but is not a stand-alone AMS Plan exercise. This annual exercise credit is only given if approved by the Area Commander to

ensure that the appropriate elements of the AMS Plan are implemented. We have changed the approval level to the Area Commander, because the Area Commander is the approval authority for the AMS Plan, not the District Commander. However, we have kept the initial review at the District Commander level in order to highlight any regional resource issues. Once we obtain sufficient experience with AMS Plan implementation, we will review the annual requirement and, if warranted, may consider revising the exercise frequency. However, to remain in compliance with our international obligations, should we deem a change to this annual frequency to be appropriate in the future, we must propose the change internationally.

Additional Changes

In addition, the part heading in this part has been amended to align with all the part headings within this subchapter. We have also corrected the Table of Contents for the entry for § 103.410, which was missing the word "Assessment."

Regulatory Assessment

This final rule is a "significant regulatory action" under section 3(f) of Executive Order 12866, Regulatory Planning and Review. The Office of Management and Budget has reviewed it under that Order. It requires an assessment of potential costs and benefits under section 6(a)(3) of that Order. It is significant under the regulatory policies and procedures of the Department of Homeland Security. A final assessment is available in the docket as indicated under **ADDRESSES**. We did not receive specific comments on the regulatory assessment for part 103. A discussion of general comments on the regulatory assessment for subchapter H can be found in the preamble of the final rule for part 101, under "Regulatory Assessment."

Cost Assessment

This rule will affect stakeholders in 47 COTP zones containing 361 ports. The regulatory assessment and analysis documentation (*see* USCG-2003-14733) details estimated costs to public and private stakeholders and does not include costs to the Coast Guard.

Because the changes in this final rule do not affect the original cost estimates presented in the temporary interim rule (68 FR 39287) (part 103), the costs remain unchanged.

The total cost estimate of the rule, as it pertains to area maritime security, is present value \$477 million (2003-2012, 7 percent discount rate). The initial cost of the startup period (June 2003-December 2003) for establishing AMS Committees and creating AMS Plans is estimated to be \$120 million (non-discounted) for all areas. Following the startup period, the first year of implementation (2004), consisting of monthly AMS Committee meetings and AMS Plan exercises and drills for all areas, is estimated to be \$106 million (non-discounted). After the first year of implementation, the annual cost of quarterly AMS Committee meetings and AMS Plan exercises and drills for all areas is estimated to be \$46 million (non-discounted). The startup period cost associated with creating AMS Committees and AMS Plans for each area is the primary cost driver of the rule. Both the startup and implementation year period (2003-2004) combined is nearly half of the total 10-year present value cost estimate, making initial development, planning, and testing the primary costs of Area Maritime Security.

This rule will require all COTPs to establish security committees, plans, training drills, and exercises for their areas, with the participation of port stakeholders in their areas. The above costs to stakeholders will be paperwork, travel, and communication costs associated with participation in AMS Plan implementation.

We estimate 1,203,200 hours of paperwork and other associated planning activities during 2003, the initial period of security meetings and development. In 2004, the first year of implementation, we estimate the value will fall slightly to 1,090,400 hours of paperwork and other related information and communication activities related to monthly AMS Committee meetings. In subsequent years, we estimate the hours will fall to 488,800 hours annually associated with AMS Committee meetings, AMS Plan revisions, and information exercises and drills.

Benefit Assessment

This final rule is one of six final rules that implement national maritime security initiatives concerning general provisions, Area Maritime Security, vessels, facilities, Outer Continental Shelf (OCS) facilities, and the 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 AMS security for the affected population reduces 135,202 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 rule				
	Vessel security	Facility security	OCS facility security	AMS	AIS
Vessels	778,633	3,385	3,385	3,385	1,317

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

Maritime entity	Annual risk points reduced by rule				
	Vessel security	Facility security	OCS facility security	AMS	AIS
Facilities	2,025	469,686	2,025
OCS facilities	41	9,903
Port Areas	587	587	129,792	105
Total	781,285	473,659	13,288	135,202	1,422

Once we determined the annual risk points reduced, we discounted these estimates to their present value (7 percent discount rate, 2003–2012) so that they could be compared to the costs. We presented the cost

effectiveness, or dollars per risk point reduced, in two ways: First, we compared the first-year cost and first-year benefit because the 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 to 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 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.

The stakeholders affected by this rule include a variety of businesses and governments. The COTP will designate approximately 200 stakeholders, per maritime area, to engage in security planning, meetings, and drills. Full participation by these stakeholders will be voluntary. We estimate the first-year cost, per stakeholder, to be \$12,800 (non-discounted). In subsequent years, the annual cost, per stakeholder (full participation in this rule), falls to \$4,940 (non-discounted).

The results from our assessment (copy available in the docket) suggest that the impact of this rule is not significant for port and maritime area authorities, owners, or operators because of the low average annual cost per stakeholder and

the voluntary nature of participating in this rule.

We estimated the majority of small entities have a less than 3 percent impact on revenue if they choose to fully participate in this rule. We anticipate the few remaining small entities that may have a greater than 3 percent impact on annual revenue will either opt out (not participate) or partially participate in the rule to the extent that the impact on revenue is not a burden.

There are other stakeholders affected by this rule in addition to port authorities, owners, and operators. The stakeholders could be any entity that the COTP invites to partially or fully participate. We anticipate the impact on other possible small entity stakeholders to be minimal because of the low average annual cost per stakeholder and the voluntary nature of participating in this rule.

Therefore, the Coast Guard certifies, under 5 U.S.C. 605(b), that this rule will not have a significant economic impact on a substantial number of small entities.

We did not receive comments regarding small entities. Additional information on small entity impacts is

available in the “Small Entities” section of the preamble for each final rule.

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 did not receive comments regarding collection of information. 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.

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.

Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular, the Act addresses actions that may result in the expenditure by a State, local, or Indian Tribal government, in the aggregate, or by the private sector of \$100,000,000 or more in any one year. This final rule is exempted from assessing the effects of the regulatory action as required by the Act because it is necessary for the national security of the United States (2 U.S.C. 1503(5)). We did not receive comments regarding the Unfunded Mandates Reform Act.

Taking of Private Property

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

Civil Justice Reform

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

Protection of Children

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

Indian Tribal Governments

This final rule does not have tribal implications under Executive Order 13175, Consultation and Coordination with Indian Tribal Governments, because it does not have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal

Government and Indian tribes. We did not receive comments regarding Indian Tribal Governments.

Energy Effects

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

This final rule has a positive effect on the supply, distribution, and use of energy. The final rule provides for security assessments, plans, procedures, and standards, which will prove beneficial for the supply, distribution, and use of energy at increased levels of maritime security. We did not receive comments regarding energy effects.

Environment

We have considered the environmental impact of this final rule and concluded that, under figure 2–1, paragraph (34)(a) and (34)(c) of Commandant Instruction M16475.ID, this rule is categorically excluded from further environmental documentation. This final rule concerns security assessments and the establishment of security committees and coordinators 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 103

Facilities, Harbors, Maritime security, Ports, Reporting and recordkeeping requirements, Security measures, Vessels, Waterways.

■ Accordingly, the interim rule adding 33 CFR part 103, that was published at 68 FR 39284 on July 1, 2003, and

amended at 68 FR 41914 on July 16, 2003, is adopted as a final rule with the following changes:

PART 103—MARITIME SECURITY: AREA MARITIME SECURITY

■ 1. The authority citation for part 103 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70102, 70103, 70104, 70112; 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 103 to read as shown above.

■ 3. In the Table of Contents, revise the entry for § 103.410 to read as follows:

§ 103.410 Persons involved in the Area Maritime Security (AMS) Assessment.

- 4. In § 103.305—
- a. Revise paragraph (a) introductory text and paragraph (a)(5), to read as set out below;
- b. Redesignate paragraph (b) as paragraph (c); and
- c. Add new paragraph (b) to read as follows:

§ 103.305 Composition of an Area Maritime Security (AMS) Committee.

(a) An AMS Committee will be composed of not less than seven members having an interest in the security of the area and who may be selected from—

* * * * *

(5) Maritime industry, including labor;

* * * * *

(b) At least seven of the members must each have 5 or more years of experience related to maritime or port security operations.

* * * * *

§ 103.500 [Amended]

■ 5. In § 103.500(b), remove the words “AMS Plans are sensitive security information and must be” and add, in their place, the words “Portions of the AMS Plan may contain sensitive security information, and those portions must be marked as such and”.

- 6. In § 103.505—
- a. Redesignate paragraphs (s), (t), and (u) as paragraphs (t), (u), and (v), respectively;
- b. In newly redesignated paragraph (u), remove the word “and”;
- c. In newly redesignated paragraph (v), remove the period and add, in its place, the word “; and”;
- d. Add new paragraphs (s) and (w) to read as follows:

§ 103.505 Elements of the Area Maritime Security (AMS) Plan.

* * * * *

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

* * * * *

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

■ 7. In § 103.515—

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

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

§ 103.515 Exercises.

* * * * *

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

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

(2) An actual increase in MARSEC Level; or

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

Dated: October 8, 2003.

Thomas H. Collins,

Admiral, Coast Guard, Commandant.

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

BILLING CODE 4910-15-U

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Parts 104, 160, and 165

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

[USCG-2003-14749]

RIN 1625-AA46

Vessel Security

AGENCY: Coast Guard, DHS.

ACTION: Final rule.

SUMMARY: This final rule adopts, with changes, the temporary interim rule published on July 1, 2003, that provides

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

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

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

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

SUPPLEMENTARY INFORMATION:

Regulatory Information

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

We received a total of 438 letters in response to the six temporary interim rules by July 31, 2003. The majority of these letters contained multiple comments, some of which applied to the

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

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

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

Background and Purpose

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

Impact on Existing Domestic Requirements

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

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

Discussion of Comments and Changes

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

Subpart A—General

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

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

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

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

interface” refers to when the vessel is at the facility or arriving at the facility.

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

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

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

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

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

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

We agree that the general reference to SOLAS is broad and could encompass

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

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

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

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

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

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

may submit for approval an Alternative Security Program to apply to vessels that operate solely on the Great Lakes and St. Lawrence Seaway.

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

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

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

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

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

be increased from 150 to 500 or, alternatively, that an exemption be added for those with fewer than 500 passengers.

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

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

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

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

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

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

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

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

We understand that ferries often function as mass transit and we have

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

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

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

Three commenters stated that the Coast Guard needs to describe how it intends to apply these regulations to

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

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

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

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

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

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

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

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

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

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

Our applicability for the security regulations in 33 CFR subchapter H is for all vessels and facilities; however, parts 104, 105, and 106 directly regulate those vessels and facilities we have determined may be involved in transportation security incidents, which does not include canoes and private residences. For example, § 104.105(a) applies to commercial vessels; therefore, a recreational boater is not regulated under part 104. If a waterfront homeowner does not meet any of the

specifications in § 105.105(a), the waterfront homeowner is not regulated under part 105. It should be noted that all waterfront areas and boaters are covered by parts 101 through 103 and, although there are no specific security measures for them in these parts, the AMS Plan may set forth measures that will be implemented at the various MARSEC Levels that may apply to them. Security zones and other measures to control vessel movement are some examples of AMS Plan actions that may affect a homeowner or a recreational boater. Additionally, the COTP may impose measures, when necessary, to prevent injury or damage or to address specific security concerns.

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

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

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

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

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

Two commenters asked whether the submission requirement for Vessel

Security Plans applies to foreign flag vessels.

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

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

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

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

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

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

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

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

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

Foreign flag vessels need not submit their Vessel Security Assessments or Vessel Security Plans to the Coast Guard for review or approval. We have revised §§ 104.115, 104.120(a)(4), and 104.410(a), to clarify that owners and operators of foreign flag vessels that meet the applicable requirements of SOLAS Chapter XI will not have to submit their assessments or plans to the Coast Guard for review or approval. These amendments also clarify that foreign vessels, which may not be subject to or operating under SOLAS, may meet these requirements through either submission to the Coast Guard or their own flag administration. Flag administrations may apply the new international security requirements to vessels other than those required to comply with SOLAS, consistent with paragraph 4.46 of part B of the ISPS Code and Resolution 7 from IMO's Diplomatic Conference on Maritime Security. Furthermore, some flag administrations not party to SOLAS may decide to apply SOLAS Chapter XI and the ISPS Code requirements to their vessels trading with the U.S. In these latter two cases—where foreign vessels not subject to SOLAS may nevertheless be required by the flag administration to comply with the requirements of SOLAS Chapter XI and the ISPS Code—the Coast Guard intends to work with the flag administration if they propose initiatives such as an Alternative

Security Program. This will likely be done through bilateral or multilateral arrangements. When no approved Alternative Security Program or bilateral arrangement exists, foreign flag vessels not subject to SOLAS covered by 33 CFR part 104 must submit their Vessel Security Assessments and Vessel Security Plans to the Coast Guard for review and approval.

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

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

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

with the requirements of SOLAS and the ISPS Code.

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

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

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

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

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

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

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

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

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

We are using the same cooperative arrangement that we have used with success in the safety realm by accepting SOLAS certificates documenting flag-state approval of foreign SOLAS Vessel Security Plans that comply with the comprehensive requirements of the ISPS Code. The consistency of the international and domestic security regimes, to the extent possible, was always a central part of the negotiations for the MTSA and the ISPS Code. In the MTSA, the Congress explicitly found that "it is in the best interests of the U.S. to implement new international instruments that establish" a maritime security system. We wholeheartedly agree and will exercise Port State Control to ensure that foreign flag vessels have approved plans and have,

in fact, implemented adequate security standards. Port State Control will not be delegated to anyone. If vessels do not meet our security requirements, we have the power to prevent those vessels from entering the U.S., and we will not hesitate to use that power in appropriate cases. The Port State Control measures will include tracking the performance of all owners, operators, flag administrations, RSOs, charterers, and port facilities. Noncompliance will subject the vessel to a range of control and compliance measures, which could include denial of entry into port or significant delay. A vessel's or foreign port facility's history of compliance, or lack thereof, or security incidents involving a vessel or port facility will be important factors in determining what actions are deemed appropriate by the Coast Guard to ensure that maritime security is preserved. The Coast Guard's current Port State Control program has been highly effective in ensuring compliance with SOLAS safety requirements, and we believe that the incorporation of the ISPS Code requirements into this program is the most efficient and effective means to carry out our Port State Control responsibilities, enhance our ability to identify substandard vessels, ensure the security of our ports, and meet the Congressional intent of the MTSA.

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

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

The Coast Guard conducts scheduled inspections during which time the Coast Guard requests and reviews documentation on board the vessel. In § 104.120(b), we require that the Vessel Security Plan and related security documentation be made available upon request to the Coast Guard during a scheduled inspection. A scheduled inspection is an inspection such as for the issuance of a Certificate of Inspection or an annual re-inspection for endorsement on a Certificate of Inspection. For uninspected vessels, we

intend to check compliance with these regulations at a frequency that is similar to those existing uninspected vessel safety programs and in conjunction with other boardings.

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

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

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

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

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

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

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

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

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

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

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

Subpart B—Vessel Security Requirements

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

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

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

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

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

and exercises. The Coast Guard intends to review these records during periodic inspections.

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

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

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

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

Nineteen commenters were concerned about the rights of seafarers at facilities. One commenter stated that the direct and specific references to shore leave in the regulations conform exactly with his position and the widespread belief that shore leave is a fundamental right of a seaman. One commenter stated that coordinating mariner shore leave with facility operators is important and should be retained, stating that shore leave for ships’ crews exists as a fundamental seafarers’ right that can be denied only in compelling circumstances. The commenter also stated that chaplains should continue to have access to vessels, especially during periods of heightened security. Four commenters requested that the

regulations require facilities to allow vessel personnel access to the facilities for shore leave, or other purposes, stating that shore leave is a basic human right and should not be left to the discretion of the terminal owner or operator. One commenter stated that seafarers are being denied shore leave as they cannot apply for visas in a timely manner and that seafarers who meet all legal requirements should be permitted to move to and from the vessel through the facility, subject to reasonable requirements in the Facility Security Plan. One commenter stated that it is the responsibility of the government to determine appropriate measures for seafarers to disembark. One commenter encouraged the government to expedite the issuance of visas for shore leave.

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

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

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

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

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

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

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

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

Sections 104.210(a)(3) and 104.215(a)(1) do not preclude an owner or operator of a company that owns vessels from appointing the same individual as both the Company Security Officer and Vessel Security Officer. The Company Security Officer may also be the Vessel Security Officer, provided he or she is able to perform the duties and responsibilities required of both positions. Generally, this provision is for vessels operating on restricted routes in a single COTP zone and for

unmanned vessels. Under § 104.215(a)(2), however, the Vessel Security Officer for manned vessels must be the Master or a member of the crew. While we are making amendments to § 104.215 to clarify security responsibilities for unmanned vessels, we are not amending this section to explicitly identify the personnel that can be designated as crew because we intended the term "crew" to be sufficiently broad and include those persons that constitute the "regular complement of the vessel." A vessel's Certificate of Inspection is issued under Title 46 of the Code of Federal Regulations and delineates crew as the vessels' complement for the safe operation and navigation of the vessel. While 33 CFR chapter I, subchapter H focuses on security, the broader interpretation of "crew" includes individuals and crew necessary for the safe operation and navigation of the vessel as well as those "persons in addition to the crew." Thus, a Certificate of Inspection need not be amended to include a reference to the Vessel Security Officer.

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

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

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

Two commenters requested amending § 104.210 regarding the duties of the

Company Security Officer to include explicit consideration of vessel-to-vessel activities.

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

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

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

B. Paragraph 13.1.3 of part B expressly states that the Company Security Officer, among other security personnel, should have knowledge of "relevant" government legislation and regulations, which clearly is not limited solely to those of the flag state.

Therefore, the requirement in the regulations reflects the international standard. Furthermore, we do prescribe additional domestic security requirements for some foreign vessels, such as cruise ships. Therefore, as a practical matter, Company Security Officers must be knowledgeable of these regulations to adequately perform their duties.

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

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

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

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

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

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

We have worked with several other Federal agencies and industry experts

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

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

We have required Vessel Security Officers on towing vessels greater than 8 meters that engage in towing barges transporting hazardous or dangerous cargos, because it is imperative that the responsibility for security on these vessels be clearly established. Recognizing that some of these towing vessels will have a small crew complement, we have not prohibited the Master from being the Vessel Security Officer. We have clarified this by amending § 104.215(a)(2) to include a specific reference to the Master. Section 104.200 provides that the Vessel Security Officer can be designated by

name or by title; therefore, we have not amended this section. The duties of the Vessel Security Officer ensure that a knowledgeable person is on board or is directly responsible for coordinating the implementation of the Vessel Security Plan. We did not intend to preclude a Company Security Officer from also serving as a Vessel Security Officer for a towing or unmanned vessel. We have amended § 104.210(a)(3) to clarify that the Company Security Officer may serve as a Vessel Security Officer, provided that he or she is able to perform the duties and responsibilities of a Company Security Officer.

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

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

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

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

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

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

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

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

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

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

We disagree with exempting ferries and their terminals from the screening requirement and, therefore, will continue to require that certain security personnel understand the various methods that could be used to conduct physical screening. Because ferries certificated to carry more than 150 passengers and the terminals that serve them may be involved in a transportation security incident, it is

imperative that security measures, such as access control, be implemented. Section 104.292 provides passenger vessels and ferries alternatives to identification checks and passenger screening. However, it does not provide alternatives to the requirements for cargo or vehicle screening. Thus, ferry security personnel assigned to screening duties should know the methods for physical screening. There is no corresponding alternative to § 104.292 for terminals serving ferries carrying more than 150 passengers; therefore, terminal security personnel assigned to screening duties should also know the methods for physical screening.

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

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

Two commenters requested that the word “seasonal” be deleted from § 104.230(b)(1) regarding requirements for drills, stating that the word

“seasonal” is irrelevant for owners and operators of uninspected vessels.

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

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

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

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

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

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

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

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

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

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

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

Sections 104.235(a) and 105.225(a) state that the records must be made available to the Coast Guard upon request, and §§ 104.235(c) and 105.225(c) state that the records must be protected from unauthorized access.

Therefore, a facility or vessel owner or operator must ensure that records are kept safely and also are available for inspection by the Coast Guard upon request, but the records do not necessarily have to be kept at the facility or on board the vessel.

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

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

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

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

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

unnecessary recordkeeping for this general "domain awareness" training.

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

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

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

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

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

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

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

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

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

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

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

MARSEC Level changes are generally issued at the Commandant level and each Marine Safety Office (MSO) will be able to disseminate them to vessel and

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

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

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

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

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

Seven commenters stated that although facility or vessel personnel need to understand the current

MARSEC Level and have a heightened state of awareness, in most cases, the specifics of the threat should not be disclosed.

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

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

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

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

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

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

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

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

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

We received two comments addressing the affects of MARSEC Level changes on the STCW and International Labor Organization (ILO) standards. One commenter asked for confirmation that implementing MARSEC Level 2 "automatically exempts vessels from the STCW and ILO work hour and rest requirements." One commenter stated

disappointment that the regulations did not address the need for increased manning at MARSEC Level 3 to ensure that personnel can perform additional duties and comply with STCW mandated rest periods.

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

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

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

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

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

We received nine comments questioning our use of the words "continuous" or "continuously" in the regulations. Four commenters requested that we amend language in § 104.245(b) by replacing the word "continuous" with the word "continual," stating that "continuous" implies that there must be constant and uninterrupted communications. One commenter requested that we amend language in § 104.285(a)(1) by replacing the word "continuously" with the word "continually," stating that "continuously" implies that there must

be constant and uninterrupted application of the security measure. One commenter requested that we amend language in § 106.275 to replace the word "continuously" with the word "frequently." One commenter recommended that instead of using the word "continuously" in § 105.275, the Coast Guard revise the definition of monitor to mean a "systematic process for providing surveillance for a facility." One commenter stated that the continuous monitoring requirements in § 106.275 place a significant burden on the owners and operators of OCS facilities because increased staff levels would be necessary to keep watch not only in the facility, but also in the surrounding area.

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

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

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

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

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

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

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

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

ensure all parties are aware of their security responsibilities.

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

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

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

As stated in §§ 104.255(e), 105.245(e), and 106.250(e), at MARSEC Levels 1 and 2, owners or operators may establish continuing Declaration of Security procedures for vessels and facilities that frequently interface with each other. These sections do not preclude owners and operators from developing Declaration of Security procedures that could apply to vessels and facilities that frequently interface. However, as stated in §§ 104.255(c) and

(d), 105.245(d), and 106.250(d), at MARSEC Level 3, all vessels and facilities required to comply with parts 104, 105, and 106 must enact a Declaration of Security agreement each time they interface. We believe that, even when under common ownership, vessels and facilities must coordinate security measures at higher MARSEC Levels and therefore should execute Declarations of Security. For MARSEC Level 1, only cruise ships and vessels carrying Certain Dangerous Cargoes (CDC) in bulk, and facilities that receive them, even when under common ownership, are required to complete a Declaration of Security each time they interface.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Coast Guard intends to coordinate with the Transportation Security Administration (TSA) and the Bureau of Customs and Border Protection (CBP) 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 CBP for the screening of international passengers and cargo. Additionally, TSA is developing a list of items prohibited from being carried on board passenger vessels.

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

We disagree with the commenter. We believe that screening of persons, their personal effects, and vehicles are necessary at all MARSEC Levels to minimize the risk of a transportation security incident. However, while we mandate that all vessels must implement screening procedures, we provide the flexibility for those vessels

to determine what those screening procedures should be, taking into account the type of vessel and the geographical region where that vessel is operating. Additionally, the intent of the regulations is that the secure area used to conduct the screening of baggage or personal effects could be the same location where the screening of persons entering the vessel takes place. Because we have kept the screening requirements in these final rules, we have also retained the provisions for designating a secure area on board the vessel or in liaison with the facility for conducting inspections and screening.

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

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

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

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

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

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

While the regulations require vessel owners and operators to deter the introduction of dangerous substances and devices, in accordance with § 104.265, the regulations do not mandate the checking of lawfully carried firearms. Our regulations are flexible to handle daily operations and allow the owners and operators to develop appropriate procedures that ensure the security of its passenger or

commercial activities. All security plans will be reviewed by the Coast Guard to ensure compliance with access control regulations.

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

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

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

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

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

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

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

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

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

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

ships," MSC/Cir.623/Rev.3, to be a useful reference in this regard. We are amending § 104.265(b) to include a verb in the sentence for clarity. We are also mirroring this clarification in §§ 105.255(b) and 106.260(b).

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

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

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

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

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

Section 104.270(d) provides a non-exhaustive list of security measures that an owner or operator may use to prevent unauthorized access to restricted areas. Only one of these measures is locking or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We disagree with the comments because the suggested changes would erode the level of security to be

achieved by the regulations by providing an unenforceable standard.

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

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

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

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

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

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

to the ferry while maintaining adequate security.

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

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

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

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

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

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

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

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

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

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

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

Two commenters encouraged the formal training of Coast Guard Port State

Control officers in enforcing these regulations to include the details of security systems and procedures, security equipment, and the elements of knowledge required of the Vessel Security Officer and Facility Security Officer.

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

Subpart C—Vessel Security Assessment (VSA)

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

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

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

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

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

Portions of security plans are sensitive security information and must be protected in accordance with 49 CFR

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

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

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

"Sensitive security information" is a designation mandated by regulations promulgated by TSA and may be found in 49 CFR part 1520. These regulations state that information designated as sensitive security information may not be shared with the general public. FOIA exempts from its mandatory release provisions those items that other laws forbid from public release. Thus, security assessments, security assessment reports, and security plans, which should be designated as sensitive security information, are all exempt from release under FOIA.

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

The MTSA requires the owners or operators of vessels that may be

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

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

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

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

We will not be providing a list of acceptable assessment companies, nor will we define "appropriate skills." It is the responsibility of the vessel or facility owner or operator to vet companies that assist them in their security assessments. In the temporary interim rule (68 FR 39254) (part 101), we stated, "we reference ISPS Code, part B, paragraph 4.5, as a list of competencies all owners and operators should use to guide their decision on hiring a company to assist with meeting the regulations. We may provide further guidance on competencies for maritime security organizations, as necessary, but do not intend to list organizations, provide standards within the regulations, or certify organizations." We require security assessments to be protected from unauthorized disclosures and will enforce this requirement,

including through the penalties provision, § 101.415.

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

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

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

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

One commenter asked whether persons who have already completed the "ISPS—Company Security Officers

Course" can be considered competent to carry out a shipboard assessment.

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

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

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

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

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

Two commenters asserted that the requirement in § 104.305(b) for an on-

scene survey to be complete and plan submitted 60 days in advance of the vessel's operation is not reasonable because the vessel's crew and equipment may not yet be on board or installed.

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

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

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

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

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

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

After further review of subpart C of parts 104, 105, and 106, we amended §§ 104.310, 105.310, and 106.310 to state that the security assessment must be reviewed and updated each time the security plan is revised and when the security plan is submitted for re-approval.

Subpart D—Vessel Security Plan (VSP)

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

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

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

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

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

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

designated and required by the Coast Guard.

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

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

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

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

We agree that a plan written in a language other than English may cause a delay during a Port State Control examination. However, we believe that all vessel personnel must have knowledge of security-related measures

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

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

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

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

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

Three commenters recommended that the regulations be amended to close "the gap" in the plan-approval process to address the period of time between December 29, 2003, and July 1, 2004. Another commenter suggested submitting the Facility Security Plan for review and approval for a new facility

“within six months of the facility owner or operator’s intent of operating it.”

We agree that the regulations do not specify plan-submission lead time for vessels, facilities, and OCS facilities that come into operation after December 29, 2003, and before July 1, 2004. The owners or operators of such vessels, facilities, and OCS facilities are responsible for ensuring they have the necessary security plans submitted and approved by July 1, 2004, if they intend to operate. We have amended §§ 104.410, 105.410, and 106.410 to clarify the plan-submission requirements for before and after July 1, 2004.

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

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

After further review of the “Submission and approval” requirements in §§ 101.120, 104.410, 105.410, and 106.410, we have amended the requirements to clarify that security plan submissions can be returned for revision during the approval process.

Thirty commenters commended the Coast Guard for providing an option for an Alternative Security Program as described in § 101.120(b) and urged the Coast Guard to approve these programs as soon as possible.

We believe the provisions in § 101.120(b) will provide greater flexibility and will help owners and operators meet the requirements of these rules. We will review Alternative Security Program submissions in a timely manner to determine if they comply with the security regulations for their particular segment. Additionally, we have amended §§ 104.410(a)(2), 105.410(a)(2), 106.410(a)(2), 105.115(a), and 106.110(a) to clarify the submission requirements for the Alternative Security Program.

We received 15 comments about the process of amending and updating the security plans. Five commenters requested that they be exempted from auditing whenever they make minimal changes to the security plans. Two commenters stated that it should not be necessary to conduct both an amendment review and a full audit of security plans upon a change in ownership or operational control. Three commenters requested a *de minimis* exemption to the requirement that

security plans be audited whenever there are modifications to the vessel or facility. Seven commenters stated that the rule should be revised to allow the immediate implementation of security measures without having to propose an amendment to the security plans at least 30 days before the change is to become effective. The commenters stated that there is something “conceptually wrong” with an owner or operator having to submit proposed amendments to security plans for approval when the amendments are deemed necessary to protect vessels or facilities.

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

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

definition for the scope of a plan change that constitutes an amendment to a Vessel Security Plan.

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

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

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

Miscellaneous

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

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

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

Regulatory Assessment

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

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

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

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

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

The estimated average incremental cost for the 15-minute update of the Vessel Security Plan accounts for the time a Company Security Officer or Vessel Security Officer spends making minor changes. The cost of an annual review and audit cost is incurred at the company, not the vessel, level. We have accounted for this cost for both large and small companies. We also assumed

that, for large companies operating vessels subject to SOLAS, the cost would be incremental to existing expenses for annual audits already required under the International Safety Management Code and other international instruments. For further detail on the cost calculations, see the Cost Assessment and Final Regulatory Flexibility Act analysis in the docket for this rule.

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

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

Cost Assessment

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

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

This assessment presents the estimated cost if vessels are operating at MARSEC Level 1, the current level of operations since the events of September 11, 2001. We also estimated

the costs for operating for a brief period at MARSEC Level 2, an elevated level of security.

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

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

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

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

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

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

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

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

associated with these conditions is \$235 million annually.

Benefit Assessment

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

measures. The difference in before and after scores indicated the benefit of the proposed action.

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

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

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

Maritime entity	Annual risk points reduced by final 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
Total	781,285	473,659	13,288	135,202	1,422

Once we determined the annual risk points reduced, we discounted these estimates to their present value (7 percent discount rate, 2003–2012) so that they could be compared to the costs. We presented the cost

effectiveness, or dollars per risk point reduced, in two ways: First, we compared the first-year cost and first-year benefit because first-year cost is the highest in our assessment as companies develop security plans and purchase

equipment. Second, we compared the 10-year present value cost and the 10-year present value benefit. The results of our assessment are presented in Table 2.

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

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

*Cost less monetized safety benefit.

Small Entities

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

We found that the facilities (part 105), vessels (part 104), and AIS rules may have a significant impact on a substantial number of small entities.

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

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

U.S. Flag SOLAS Vessels.

We estimated that 88 companies that own U.S. flag SOLAS vessels will be

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

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

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

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

Domestic Vessels

We estimated that 1,683 companies that own domestic vessels will be

affected by the final rule. We researched these companies and found revenue data for 822 of them (49 percent). The revenue impacts for these vessels are presented in Table 4. As with U.S. flag SOLAS vessels, we considered the impacts to small businesses during the first year of implementation, when

companies will be conducting assessments, developing security plans, and purchasing equipment. We also considered annual revenue impacts following the first year, when companies will have the assessments and plans complete, but will need to conduct quarterly drilling.

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

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

We assumed that the remaining 861 entities that did not have revenue data

are very small businesses. We assumed

that the final rule may have a significant economic impact on these businesses.

Assistance for Small Entities

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

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

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

Collection of Information

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

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

Federalism

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

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

Additionally, the Coast Guard has reviewed the MTSA with a view to whether we may construe it as non-preemptive of State authority over the same subject matter. We have determined that it would be inconsistent with the federalism principles stated in the Executive Order to construe the MTSA as not preempting State regulations that conflict with the regulations in this final rule. This is because owners or operators of facilities and vessels—that are subject to the requirements for conducting security assessments, planning to secure their facilities and vessels against threats revealed by those assessments, and complying with the standards, both performance and specific construction, design, equipment, and operating requirements—must have one uniform, national standard that they must meet. Vessels and shipping companies, particularly, would be confronted with an unreasonable burden if they had to comply with varying requirements as they moved from State to State. Therefore, we believe that the

federalism principles enumerated by the Supreme Court in *U.S. v. Locke*, 529 U.S. 89 (2000) regarding field preemption of certain State vessel safety, equipment, and operating requirements extends equally to this final rule, especially regarding the longstanding history of significant Coast Guard maritime security regulation and control of vessels for security purposes. But, the same considerations apply to facilities, at least insofar as a State law or regulation applicable to the same subject for the purpose of protecting the security of the facility would conflict with a Federal regulation; in other words, it would either actually conflict or would frustrate an overriding Federal need for uniformity.

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

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

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

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

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

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

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

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

The implementation timeline of these final rules follows the mandates of the

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

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

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

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

the scope of vehicle screening required under the regulations.

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

Unfunded Mandates Reform Act

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

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

Taking of Private Property

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

Civil Justice Reform

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

Protection of Children

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

Indian Tribal Governments

This final rule does not have tribal implications under Executive Order

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

Energy Effects

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

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

We did not receive comments regarding energy effects.

Environment

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

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

We did not receive comments regarding the environment.

List of Subjects

33 CFR Part 104

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

33 CFR Part 160

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

33 CFR Part 165

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

46 CFR Part 2

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

46 CFR Part 31

Cargo vessels, Inspection and certification, Maritime security.

46 CFR Part 71

Inspection and certification, Maritime security, Passenger vessels.

46 CFR Part 91

Cargo vessels, Inspection and Certification, Maritime security.

46 CFR Part 115

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

46 CFR Part 126

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

46 CFR Part 176

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

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

33 CFR Chapter I

PART 104—MARITIME SECURITY: VESSELS

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

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

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

■ 3. In § 104.105—

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

■ b. Add new paragraph (a)(11); and

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

§ 104.105 Applicability.

(a) * * *

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(iv) Provides emergency assistance.

* * * * *

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

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

* * * * *

■ 4. Revise § 104.110 to read as follows:

§ 104.110 Exemptions.

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

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

■ 5. Revise § 104.115 to read as follows:

§ 104.115 Compliance dates.

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

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

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

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

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

(1) Vessels subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI, must carry on board a valid International Ship Security Certificate that certifies that the verifications required by part A, Section 19.1, of the International Ship and Port Facility Security (ISPS) Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed. This includes ensuring that the vessel meets the applicable requirements of SOLAS Chapter XI-2 (Incorporated by reference, see

§ 101.115 of this chapter) and the ISPS Code, part A, having taken into account the relevant provisions of the ISPS Code, part B, and that the vessel is provided with an approved security plan.

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

■ 6. In § 104.120—

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

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

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

§ 104.120 Compliance documentation.

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

* * * * *

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

* * * * *

■ 7. Revise § 104.125 to read as follows:

§ 104.125 Noncompliance.

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

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

§ 104.140 Alternative Security Programs.

* * * * *

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

* * * * *

■ 9. In § 104.200—

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

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

§ 104.200 Owner or operator.

* * * * *

(b) * * *

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

* * * * *

§ 104.205 [Amended]

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

§ 104.210 [Amended]

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

§ 104.215 [Amended]

■ 12. In § 104.215—

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

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

§ 104.225 [Amended]

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

■ 14. In § 104.230—

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

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

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

§ 104.230 Drill and exercise requirements.

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

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

(b) * * *

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

* * * * *

§ 104.235 [Amended]

■ 15. In § 104.235—

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

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

■ 16. In § 104.240—

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

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

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

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

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

* * * * *

(b) * * *

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

* * * * *

■ 17. In § 104.255—

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

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

§ 104.255 Declaration of Security (DoS).

* * * * *

(b) * * *

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

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

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

* * * * *

§ 104.265 [Amended]

■ 18. In § 104.265—

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

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

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

■ d. In paragraph (c)(5), remove the word “seafarer’s” and add, in its place, the word “seafarers’”;

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

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

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

§ 104.275 [Amended]

■ 19. In § 104.275—

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

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

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

■ d. Remove paragraph (a)(6);

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

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

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

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

§ 104.285 [Amended]

■ 20. In § 104.285—

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

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

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

■ 21. In § 104.292—

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

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

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

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

§ 104.292 Additional requirements—passenger vessels and ferries.

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

§ 104.297 [Amended]

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

§ 104.300 [Amended]

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

§ 104.305 [Amended]

■ 24. In § 104.305—
 ■ a. In the introductory text to paragraphs (d)(3), (d)(4), and (d)(5), after the word “VSA”, add the word “report”;
 ■ b. In § 104.305(d)(3)(iv) after the words “dangerous goods” remove the word “or” and replace with the word “and”; and
 ■ c. Redesignate paragraph (d)(6) as paragraph (e) and, in the second sentence, after the words “The VSA”, add the words “, the VSA report.”
 ■ 25. Add § 104.310(c) to read as follows:

§ 104.310 Submission requirements.

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

§ 104.400 [Amended]

■ 26. In § 104.400—
 ■ a. In paragraph (a)(2), after the words “Must be written in English” add the words “, although a translation of the VSP in the working language of vessel personnel may also be developed”.
 ■ b. Revise paragraph (b) to read as follows:

§ 104.400 General.

(b) The VSP must be submitted to the Commanding Officer, Marine Safety Center (MSC) 400 Seventh Street, SW., Room 6302, Nassif Building, Washington, DC 20590-0001, in a written or electronic format. Information for submitting the VSP electronically can be found at <http://www.uscg.mil/HQ/MSC>. Owners or operators of foreign flag vessels that are subject to SOLAS

Chapter XI must comply with this part by carrying on board a valid International Ship Security Certificate that certifies that the verifications required by Section 19.1 of part A of the ISPS Code (Incorporated by reference, see § 101.115 of this subchapter) have been completed. As stated in Section 9.4 of the ISPS Code, part A requires that, in order for the ISSC to be issued, the provisions of part B of the ISPS Code need to be taken into account.

- 27. In § 104.410—
- a. Revise the introductory text for paragraph (a) to read as set out below;
- b. In paragraph (a)(1), after the words “Vessel Security Plan (VSP)”, add the words “, in English,”;
- c. Revise paragraphs (a)(2) and (b) to read as set out below;
- d. In paragraph (c)(1), remove the words “, or” and add, in their place, a semicolon;
- e. Redesignate paragraph (c)(2) as paragraph (c)(3);
- f. Add new paragraph (c)(2) to read as follows:

§ 104.410 Submission and approval.

(a) In accordance with § 104.115, on or before December 31, 2003, each vessel owner or operator must either:
 (2) If intending to operate under an Approved Security Program, a letter signed by the vessel owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

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

(c) 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.

(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 "vitaly 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 (CBP) 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 CBP 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 cargoes 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 MTTSA 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 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 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 CBP 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 M16475.1D, 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 its 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)	<h2 style="margin:0;">FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY</h2>	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)																				
<table style="width:100%; border:none;"> <tr> <td><input type="checkbox"/> Break Bulk</td> <td><input type="checkbox"/> Petroleum</td> <td><input type="checkbox"/> Certain Dangerous Cargo</td> <td><input type="checkbox"/> Passengers (Subchapter H)</td> <td><input type="checkbox"/> If other, explain below:</td> </tr> <tr> <td><input type="checkbox"/> Dry Bulk</td> <td><input type="checkbox"/> Chemical</td> <td><input type="checkbox"/> Barge Fleeting</td> <td><input type="checkbox"/> Passengers (Ferries)</td> <td rowspan="3" style="border: 1px solid black; width: 150px; height: 30px;"></td> </tr> <tr> <td><input type="checkbox"/> Container</td> <td><input type="checkbox"/> LHG/LNG</td> <td><input type="checkbox"/> Offshore Support</td> <td><input type="checkbox"/> Passengers (Subchapter K)</td> </tr> <tr> <td><input type="checkbox"/> RO-RO</td> <td><input type="checkbox"/> Explosives and other dangerous cargo</td> <td><input type="checkbox"/> Military Supply</td> <td></td> </tr> </table>			<input type="checkbox"/> Break Bulk	<input type="checkbox"/> Petroleum	<input type="checkbox"/> Certain Dangerous Cargo	<input type="checkbox"/> Passengers (Subchapter H)	<input type="checkbox"/> If other, explain below:	<input type="checkbox"/> Dry Bulk	<input type="checkbox"/> Chemical	<input type="checkbox"/> Barge Fleeting	<input type="checkbox"/> Passengers (Ferries)		<input type="checkbox"/> Container	<input type="checkbox"/> LHG/LNG	<input type="checkbox"/> Offshore Support	<input type="checkbox"/> Passengers (Subchapter K)	<input type="checkbox"/> RO-RO	<input type="checkbox"/> Explosives and other dangerous cargo	<input type="checkbox"/> Military Supply	
<input type="checkbox"/> Break Bulk	<input type="checkbox"/> Petroleum	<input type="checkbox"/> Certain Dangerous Cargo	<input type="checkbox"/> Passengers (Subchapter H)	<input type="checkbox"/> If other, explain below:																
<input type="checkbox"/> Dry Bulk	<input type="checkbox"/> Chemical	<input type="checkbox"/> Barge Fleeting	<input type="checkbox"/> Passengers (Ferries)																	
<input type="checkbox"/> Container	<input type="checkbox"/> LHG/LNG	<input type="checkbox"/> Offshore Support	<input type="checkbox"/> Passengers (Subchapter K)																	
<input type="checkbox"/> RO-RO	<input type="checkbox"/> Explosives and other dangerous cargo	<input type="checkbox"/> Military Supply																		
VULNERABILITY AND SECURITY MEASURES																				
7a. Vulnerability		7b. Vulnerability Category																		
		<input type="checkbox"/> If other, explain																		
8a. Selected Security Measures (MARSEC Level 1)		8b. Security Measures Category																		
		<input type="checkbox"/> If other, explain																		
9a. Selected Security Measures (MARSEC Level 2)		9b. Security Measures Category																		
		<input type="checkbox"/> If other, explain																		
10a. Selected Security Measures (MARSEC Level 3)		10b. Security Measures Category																		
		<input type="checkbox"/> If other, explain																		
VULNERABILITY AND SECURITY MEASURES																				
7a. Vulnerability		7b. Vulnerability Category																		
		<input type="checkbox"/> If other, explain																		
8a. Selected Security Measures (MARSEC Level 1)		8b. Security Measures Category																		
		<input type="checkbox"/> If other, explain																		
9a. Selected Security Measures (MARSEC Level 2)		9b. Security Measures Category																		
		<input type="checkbox"/> If other, explain																		
10a. Selected Security Measures (MARSEC Level 3)		10b. Security Measures Category																		
		<input type="checkbox"/> If other, explain																		

DEPARTMENT OF HOMELAND SECURITY**Coast Guard****33 CFR Part 106**

[USCG-2003-14759]

RIN 1625-AA68

Outer Continental Shelf 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 mobile offshore drilling units (MODUs) not subject to the International Convention for the Safety of Life at Sea, 1974, and certain fixed and floating facilities on the Outer Continental Shelf (OCS) other than deepwater ports. This rule also requires the owners or operators of OCS facilities to designate security officers for OCS facilities, develop security plans based on security assessments and surveys, implement security measures specific to the OCS facility's operation, and comply with Maritime Security Levels. This rule is one in a series of final rules on maritime security in today's **Federal Register**. To best understand this rule, first read the final rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792), published elsewhere in today's **Federal Register**.

DATES: This final rule is effective November 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-2003-14759 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 Greg Versaw (G-MPS-2), U.S. Coast Guard by telephone 202-267-4144 or by electronic mail gversaw@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 "Outer Continental Shelf Facility Security" in the **Federal Register** (68 FR 39338). 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 "Outer Continental Shelf 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 rule. Because of statutorily imposed time constraints for publishing these regulations, we were unable to consider comments received after the period for receipt of comments closed on July 31, 2003.

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

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

Background and Purpose

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

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 106.

Two commenters proposed language to clarify the definition of "OCS facility" to make clear that the term includes Mobile Offshore Drilling Units (MODUs) when attached to the subsoil or seabed for the exploration, development, or production of oil or natural gas. One commenter suggested that this additional language would "provide clarification regarding the applicability of" part 106.

The purpose of the broad definition of "OCS facility" in § 101.105 is to ensure that OCS facilities that are not regulated under part 106 will be covered by parts 101 through 103. The proposed additional language would not add clarity to part 106 because the applicability in § 106.105 states that the section applies only to those MODUs that are operating for the purposes of engaging in the exploration, development, or production of oil, natural gas, or mineral resources.

Two commenters suggested amending the definition of "owner or operator" so

that the definition includes, for OCS facilities: “the lessee or the operator designated to act on behalf of the lessee in accordance with 30 CFR part 250.” One commenter sought clarification of the terms “owner or operator” and suggested adding “operational control is the ability to influence or control the physical or commercial activities pertaining to that facility for any period of time.”

We disagree with adding the suggested language of the first commenter because we have concluded that the person with operational control is the best person to implement these regulations and, therefore, should be responsible for implementation. The language proposed would include a lessee regardless of whether or not that lessee maintains such operational control. We also disagree with adding the suggested language of the second comment because it would be unnecessarily limiting.

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

With regard to the definition of “facility” and the suggested additional language regarding MODUs, the definition clearly incorporates MODUs that are not covered under part 104 and MODUs that are sufficiently covered under parts 101 through 103 and 106. Therefore, we are not amending our definition of facility nor incorporating the suggested explicit exemption from part 105 because these MODUs are excluded. We have, however, amended the applicability section of part 104 (§ 104.105) so that foreign flag, non-self propelled MODUs that meet the threshold characteristics set for OCS facilities are regulated by 33 CFR part 106, rather than 33 CFR part 104. We have done so because MODUs act and function more like OCS facilities, have limited interface activities with foreign

and U.S. ports, and their personnel undergo a higher level of scrutiny to obtain visas to work on the Outer Continental Shelf. These amendments to § 104.105 required us to add a definition for “cargo vessel” in § 101.105. With these changes, we believe the existing definitions of “facility” and “OCS facility” in § 101.105 are sufficient to conclusively identify those entities that are subject to parts 104, 105, and 106. In addition, the definition of “OCS facility,” as written, ensures that these entities will be subject to relevant elements of an OCS Area Maritime Security (AMS) Plan. We believe the language in § 106.105, read in concert with the amended § 104.105(a)(1), and the existing definitions in part 101, is sufficient to preclude MODUs that are in compliance with part 104 from being subject to part 106.

We received four comments on the applicability of part 106 to certain OCS facilities. Three commenters stated that the operating conditions referenced in § 106.105 should remain as written. A fourth commenter stated that the size criteria used in § 106.105 contains no support; that the regulations are a duplication of existing informal security measures; that the regulations do not define “adequate level of security” and offer no support that scrutiny of personnel and cargo will, or has in the past, prevented terrorist attacks; that the rule imposes a huge paperwork and formal reporting burden; that training of employees to detect dangerous situations and devices on facilities located more than 100 miles from shore is unreasonable; that the security provided by the Declaration of Security is minimal; that there is no need for the OCS Facility Security Assessment; and that the OCS Facility Security Plan will offer no security from exterior threats.

As discussed in the temporary interim rule titled “Implementation of National Maritime Security Initiatives” (68 FR 39250), we determined the applicability of part 106 for those facilities that may be involved in a transportation security incident. In developing part 106 and the security measures in it, we deliberately reviewed and incorporated much of the pre-existing informal security measures to ensure standardization and minimize the burden to those in industry that have already voluntarily adopted standards. We have determined that the security measures in part 106 will reduce the likelihood of a transportation security incident by increasing the awareness of security threats to the OCS facility. We believe that the best means of deterring incidents is to reduce the vulnerabilities of the OCS facility to a security threat by ensuring that the

owner or operator of that OCS facility increases their vigilance, awareness, and control over the vessels and persons that interact with the OCS facility. The OCS Facility Security Assessment and Plan are not envisioned to be the sole means of deterrence against security incidents. All of the security plans of the National Maritime Security Initiatives work in conjunction to reduce the vulnerability of the Marine Transportation System from various types of attacks originating from air, land, and sea. We recognize that we impose a requirement for the submission of assessments and plans to ensure compliance. To reduce the overall paperwork burden, we allow a single plan to cover multiple OCS facilities.

After further review of § 106.105 and discussion with the Minerals Management Service (MMS), we have determined that there may be OCS facilities acting as “hubs” for oil transportation that do not meet the production characteristics that are regulated under this part. However, due to unique local conditions, specific intelligence information, or other identifiable and articulable risk factors, these “hub” facilities may be involved in a transportation security incident. Therefore, on a case-by-case basis, these “hub” facility operations will be reviewed and, if appropriate, a MARSEC Directive will be issued to address these circumstances.

One commenter asked how OCS facilities not directly regulated under part 106 would be regulated.

As indicated in § 103.100, all facilities located in waters subject to the jurisdiction of the U.S. are covered by part 103 and must comply with the requirements in the AMS Plan, as developed by the AMS Committee.

Six commenters requested that the Coast Guard establish, without delay, an AMS Committee for the OCS portion of the Gulf of Mexico as an essential step in moving the various Federal law enforcement agencies and industry toward a mutual understanding of the response to a transportation security incident on the OCS.

We intend to cover the OCS facilities in the Gulf of Mexico by a single, District-wide AMS Plan. The establishment of an AMS Committee for the OCS facilities in the Gulf of Mexico was discussed at recent Gulf Safety Committee and National Offshore Safety Advisory Committee (NOSAC) meetings. We intend to form an AMS Committee for this area in the near future. Additionally, owners and operators of OCS facilities are encouraged to participate on the AMS

Committee of the COTP zone that is most relevant to their operations.

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 Maritime Transportation Security Act of 2002 (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 allowed. 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.

We are amending the dates of compliance in § 106.110(a) and (b), § 106.115, and § 106.410(a) to align with the MTSA and the International Ship and Port Facility Security Code (ISPS Code) compliance dates.

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 not 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.

Two commenters stated that in its control and compliance measures, the Coast Guard should clarify its legal authority to establish a security zone beyond its territorial sea.

One basis for the Coast Guard to establish security zones in the Exclusive Economic Zone (EEZ) is pursuant to the Ports and Waterways Safety Act, 33 U.S.C. 1221 *et seq.* For example, consistent with customary international law, 33 U.S.C. 1226 provides the Coast Guard with authority to carry out or require measures, including the establishment of safety and security

zones, to prevent or respond to an act of terrorism against a vessel or public or commercial structure that is located within the marine environment. 33 U.S.C. 1222 defines "marine environment" broadly to include the waters and fishery resources of any area over which the United States asserts exclusive fishery management authority. The United States asserts exclusive fishery management authority in the EEZ.

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 and facility 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 equivalencies 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 through 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.

Subpart B—Outer Continental Shelf (OCS) Facility Security Requirements

This subpart describes the responsibilities of the facility owner or operator and personnel relative to OCS facility security. It includes requirements for training, drills, recordkeeping, and Declarations of Security. It identifies specific security measures, such as those for access

control, restricted areas, and monitoring.

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

We cannot establish only guidelines because the MTSA and the International Convention for Safety of Life at Sea, 1974 (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.

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 the Facility Security Officer. In addition, MARAD intends to develop course approval and certification requirements in the near future.

In the final rule for "Vessel Security" published elsewhere in today's **Federal Register** we made amendments to the responsibilities of the Company Security Officer. In this final rule, we are making conforming amendments to § 106.205(a)(2) to clarify that the Company Security Officer may also perform the duties of a Facility Security Officer.

Nine commenters requested formal alternatives to Facility Security Officers, Company Security Officers, and Vessel Security Officers much like the requirements of the Oil Pollution Act of 1990, that 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.

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.

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.

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).

We received 28 comments regarding communication of changes in the MARSEC Levels. Most commenters were concerned about the Coast Guard's capability to communicate timely changes in MARSEC Levels to facilities and vessels. Some stressed the importance of MARSEC Level information reaching each port area in the COTP's zone and the entire maritime industry. Some stated that local Broadcast Notice to Mariners and MARSEC Directives are flawed methods of communication and stated that the only acceptable means to communicate changes in MARSEC Levels, from a timing standpoint, are via 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 means. Communication of MARSEC Levels will be done in the most expeditious means available, given the characteristics of the port and its operations. These means will be outlined in the AMS Plan and exercised to ensure vessel and facility owners and operators, or their designees, are able to quickly communicate with us and vice-versa. Because MARSEC Directives will not be as expeditiously communicated as other COTP Orders and are not meant to communicate changes in MARSEC Levels, we have amended § 101.300 to remove the reference to MARSEC Directives.

Two commenters requested that § 104.240(a) and (b)(1) be amended to specify that vessels must implement appropriate security measures before interfacing with facilities that are not located in a port. We agree that the vessel owner or operator, once notified of a change in MARSEC Level, must implement appropriate security measures before interfacing with a

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

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 that operates regularly 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 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) 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 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 will amend § 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).

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

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

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 §§ 106.250 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.

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

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

Two commenters asked us to amend § 106.250(f) to clarify that an expired Declaration of Security (§ 106.250(e)(2) or (e)(3)) must be replaced by a new Declaration of Security, in order for there to be a valid Declaration of Security.

Although we agree that an expired Declaration of Security must be replaced by a new Declaration of Security, in order for there to be a valid Declaration of Security, we believe that § 106.250 needs no further clarification. We do not preclude an OCS facility from executing a new Declaration of Security in accordance with § 106.250.

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.

Eight commenters suggested that access control on board 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 OCS 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.

We are amending § 104.265(b) to include a verb in the sentence for clarity. We are also mirroring this clarification in §§ 105.255(b) and 106.260(b).

We are amending § 106.265(c) to clarify the requirement by removing an extraneous word.

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) which 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.

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 stated that the provision to mandate restricted areas on board OCS facilities should be removed from the rule, arguing that limiting access during an emergency should not be tolerated.

If the security assessment and plan for the OCS facility does not take into account access to restricted areas during an emergency situation, it may hinder effective response. Therefore, we have included several provisions to ensure that the security assessment and plan for the OCS facility address this issue, such as in §§ 106.205(d)(10), 106.280(b), and 106.305(c)(1)(vii).

One commenter suggested that this regulation contain provisions to allow vessels to continue fishing in or around OCS facilities. The commenter was concerned that any effort to prevent access to areas around these facilities would cause severe economic hardship to a large number of charterboat businesses.

The security regulations do not contain any provisions that specifically restrict fishing around OCS facilities. The OCS facility owner or operator may, however, restrict some areas as part of the facility's security measures. We do not believe that part 106 will cause a hardship for vessels that fish around OCS facilities because part 106 regulates only approximately 1 percent of all

those facilities and because such restricted areas will likely be designated only during periods of heightened security.

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

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

Subpart C—Outer Continental Shelf (OCS) 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 under §§ 104.400(c), 105.400(c), and 106.400(c). We are also 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 sensitive security information portions of the security plans. In accordance with 49 CFR part 1520 and pursuant to 5 U.S.C. 552(b)(3), sensitive security information is exempt from disclosure under FOIA. 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.

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 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 potential conflicts between security plans and the AMS Plan will be identified during the Facility Security Plan approval process.

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 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.

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

We will not be providing a list of acceptable assessment companies, nor will we define “appropriate skills.” It is the responsibility of the vessel or facility owner or operator to vet companies that assist them in their security assessments. In the temporary interim rule (68 FR 39254) (part 101), we stated, “we reference ISPS Code, part B, paragraph 4.5, as a list of competencies all owners and operators should use to guide their decision on hiring a company to assist with meeting the regulations. We may provide further guidance on competencies for maritime security organizations, as necessary, but do not intend to list organizations, provide standards within the regulations, or certify organizations.” We require security assessments to be protected from unauthorized disclosures

and will enforce this requirement, including through the penalties provision under § 101.415.

After further review of subpart C of parts 104, 105, and 106, 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 reapproval.

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—Outer Continental Shelf (OCS) Facility Security Plan (FSP)

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

One commenter recommended that the interval for audits of the OCS Facility Security Plan be changed to biennial to be consistent with the audit requirements for emergency response plans.

The annual audit certifies that the OCS Facility Security Plan continues to meet the applicable requirements of part 106. We believe that annual audits are necessary because the OCS Facility Security Plan, as a living document, should be continuously updated to incorporate changes or lessons learned from drills and exercises.

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 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.

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

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.

Additional Changes

During our review of this part, we noted that a section required a non-substantive editorial change, such as accurately completing a list. The section is § 106.275(a)(1). In addition, the part heading in this part has been amended to align with all the part headings within this subchapter.

Regulatory Assessment

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

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

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

Cost Assessment

For the purposes of good business practice or pursuant to regulations promulgated by other Federal and State agencies, many companies already have spent a substantial amount of money and resources to upgrade and improve security. The costs shown in this assessment do not include 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 39341) (part 106), the costs remain unchanged.

The Coast Guard realizes 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, the Coast Guard assumes that each company will implement this final rule differently based on the types of OCS facilities it owns or operates and whether it engages in international or domestic trade.

This final rule will affect about 40 OCS facilities under U.S. jurisdiction, (current and future OCS facilities). These OCS facilities engage in exploring for, developing, or producing oil, natural gas, or mineral resources. To determine the number of OCS facilities, we used data that the Mineral Management Service (MMS) has identified as nationally critical OCS oil and gas infrastructure. These OCS facilities meet or exceed any of the following operational threshold characteristics:

- (1) OCS facility hosts more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more;
- (2) Production greater than 100,000 (one hundred thousand) barrels of oil per day; or

- (3) Production greater than 200,000,000 (two hundred million) cubic feet of natural gas per day.

The estimated cost of complying with the final rule is present value \$37 million (2003–2012, 7 percent discount rate). In the first year of compliance, the cost of security assessments and plans, training, personnel, and paperwork is an estimated \$3 million (non-discounted). Following initial implementation, the annual cost of compliance is an estimated \$5 million (non-discounted).

Approximately 80 percent of the initial cost of the final rule is for assigning and establishing Company Security Officers and Facility Security Officers, 12 percent is associated with paperwork creating Facility Security Assessments and Facility Security Plans, and 8 percent of the cost is associated with initial training (not including quarterly drills). Following the first year, approximately 58 percent of the cost is training (including quarterly drills), 42 percent is for Company Security Officers and Facility Security Officers, and less than 1 percent is associated with paperwork. Annual training (including quarterly drills) is the primary cost driver of OCS facility security.

We estimated approximately 3,200 burden hours for paperwork during the first year of compliance (40 hours for each Facility Security Assessment and each Facility Security Plan). We estimated approximately 160 burden hours annually following full implementation of the final rule to update Facility Security Assessments and Facility Security Plans.

We estimated the cost of this final rule to be minimal in comparison to vessel and non-OCS facility security implementation. This final rule includes only personnel, training, and paperwork costs for the affected OCS facility population. We assume the industry is adequately prepared with equipment suited to be used for security purposes (lights, radios, communications), therefore no security equipment installation, upgrades, or maintenance will be required for this final rule.

Benefit Assessment

This final rule is one of six final rules that implement national maritime security initiatives concerning General Provisions, Area Maritime Security, Vessels, Facilities, OCS Facilities, and AIS. The Coast Guard used the National Risk Assessment Tool (N-RAT) to assess benefits that would result from increased security for vessels, facilities, OCS facilities, and areas. The N-RAT considers threat, vulnerability, and consequences for several maritime

entities in various security-related scenarios. For a more detailed discussion on the N-RAT and how we employed this tool, refer to "Applicability of National Maritime Security Initiatives" in the temporary interim rule titled "Implementation of National Maritime Security Initiatives" (68 FR 39243) (part 101). For this benefit assessment, the Coast Guard used a team to calculate a risk score for each entity and scenario before and after the implementation of required security measures. The difference in before and

after scores indicated the benefit of the proposed action.

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

National Maritime Security Initiatives" (68 FR 39274) (part 101).

The Coast Guard determined annual risk points reduced for each of the 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 OCS facility security for the affected population reduces 13,288 risk points annually through 2012. The benefits attributable for part 101, General Provisions, were not considered separately because 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
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), the Coast Guard has 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. The Coast Guard has 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**.

There are approximately 40 total current and future OCS facilities owned by five large companies that will be affected by this final rule. Depending on how the corporate headquarters' operation is classified and whether it is oil or gas specific, these companies are generally classified under the North American Industry Classification System (NAICS) code 211111 or 221210. According to the Small Business Administration guidelines for these

industries, a company with less than 500 total corporate employees is considered a small entity. The entities affected by this final rule do not qualify as small entities because all of them have more than 500 employees.

Therefore, the Coast Guard certifies under 5 U.S.C. 605(b) that this final rule will not have a significant economic impact on a substantial number of small entities.

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.

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.

Unfunded Mandates Reform Act

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

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

Taking of Private Property

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

Civil Justice Reform

This final rule meets applicable standards in sections 3(a) and 3(b)(2) of

Executive Order 12988, Civil Justice Reform, to minimize litigation, eliminate ambiguity, and reduce burden. We did not receive comments regarding Civil Justice Reform.

Protection of Children

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

Indian Tribal Governments

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

Energy Effects

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

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

We did not receive comments regarding energy effects.

Environment

We have considered the environmental impact of this final rule and concluded that under figure 2–1, paragraph (34)(a) and (34)(c), of

Commandant Instruction M16475.ID, this final rule is categorically excluded from further environmental documentation. This final rule concerns security assessments, plans, training for personnel, and the establishment of security positions that will contribute to a higher level of marine safety and security for OCS facilities extracting oil or gas. 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 106

Facilities, Maritime security, Outer Continental Shelf, Reporting and recordkeeping requirements, Security measures.

■ Accordingly, the interim rule adding 33 CFR part 106, that was published at 68 FR 39338 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 106—MARITIME SECURITY: OUTER CONTINENTAL SHELF (OCS) FACILITIES

■ 1. The authority citation for part 106 continues to read as follows:

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

- 2. Revise the heading to part 106 to read as shown above.
- 3. In § 106.110—
 - a. Revise paragraph (a) to read as set out below; and
 - b. In paragraph (b), remove the date "June 25, 2004" and add, in its place, the date "July 1, 2004":

§ 106.110 Compliance dates.

(a) On or before December 31, 2003, OCS facility owners or operators must submit to the cognizant District Commander for each OCS 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 OCS facility owner or operator stating which approved

Alternative Security Program the owner or operator intends to use.

* * * * *

§ 106.115 [Amended]

- 4. In § 106.115—
 - a. In the introductory text, remove the words “that no later than” and add, in their place, the word “before”; and
 - b. In paragraph (c), after the words “a copy of the Alternative Security Program the OCS 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,”.
- 5. Revise § 106.120 to read as follows:

§ 106.120 Noncompliance.

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

- 6. In § 106.200—
 - a. In paragraph (b)(7), remove the word “and”;
 - b. In paragraph (b)(8), remove the period and add, in its place, the words “; and”; and
 - c. Add paragraph (b)(9) to read as follows:

§ 106.200 Owner or operator.

* * * * *

- (b) * * *
 - (9) Ensure consistency between security requirements and safety requirements.

§ 106.205 [Amended]

- 7. In § 106.205(a)(2), after the word “organization”, add the words “, including the duties of a Facility Security Officer”.

§ 106.220 [Amended]

- 8. In § 106.220, in the introductory paragraph, after the words “of the following”, add the words “, as appropriate”.
- 9. Revise § 106.225(a) to read as follows:

§ 106.225 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 FSO reports attainment to the cognizant District Commander.

* * * * *

§ 106.230 [Amended]

- 10. In § 106.230(b)(1), remove the words “each security training session” and add, in their place, the words “training under § 106.215”.

§ 106.250 [Amended]

- 11. In § 106.250, in paragraph (d)—
 - a. After the words “part 104”, add the words “of this chapter, or their designated representatives,”; and
 - b. After the word “DoSs”, add the words “as required in paragraphs (b)(1) and (b)(2) of this section”.

§ 106.260 [Amended]

- 12. In § 106.260—
 - a. In paragraph (b) introductory text, after the words “ensure that”, add the words “the following are specified”;
 - b. In paragraph (b)(3), remove the words “are established”; and
 - c. In paragraph (c)(2), after the word “vessels”, add the words “or other transportation conveyances”.

§ 106.265 [Amended]

- 13. In § 106.265(c), remove the words “should include” and add, in their place, the word “includes”.

§ 106.275 [Amended]

- 14. In § 106.275—
 - a. In paragraph (a)(1), after the word “patrols”, remove the word “and” and add, in its place, a comma; and
 - b. In paragraph (b)(4), remove the word “continually” and add, in its place, the word “continuously”.
- 15. In § 106.305—
 - a. Revise paragraph (c)(2)(v) to read as set out below; and
 - b. Add paragraphs (d)(3), (d)(4), (d)(5), and (e) to read as follows:

§ 106.305 Facility Security Assessment (FSA) requirements.

* * * * *

- (c) * * *
 - (2) * * *
 - (v) Effects of a nuclear, biological, radiological, explosive, or chemical attack to the OCS facility’s shoreside support system;
- * * * * *
- (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) OCS facility personnel;
 - (ii) Visitors, vendors, repair technicians, vessel personnel, etc.;

- (iii) OCS facility stores;
 - (iv) Any security communication and surveillance systems; and
 - (v) Any other 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 personnel duties and security assignments;
 - (iii) The impact of watch-keeping duties and risk of fatigue on 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 OCS facility measures and operations, including—

- (i) Ensuring performance of all security duties;
 - (ii) Controlling access to the OCS facility through the use of identification systems or otherwise;
 - (iii) Controlling the embarkation of OCS facility personnel and other persons and their effects (including personal effects and baggage, whether accompanied or unaccompanied);
 - (iv) Supervising the delivery of stores and industrial supplies;
 - (v) Monitoring restricted areas to ensure that only authorized persons have access;
 - (vi) Monitoring deck areas and areas surrounding the OCS facility; 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.

■ 16. In § 106.310—

- a. In paragraph (a), remove the words “§ 106.405 of this part” and add, in their place, the words “§ 106.410 of this part”; and
- b. Add paragraph (c) to read as follows:

§ 106.310 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.
- 17. In § 106.410, revise paragraph (a), introductory text, and paragraphs (a)(2), (b), and (c) to read as follows:

§ 106.410 Submission and approval.

- (a) On or before December 31, 2003, the owner or operator of each OCS facility currently in operation must either:
 - * * * * *
 - (2) If intending to operate under an Approved Security Program, submit a

letter signed by the OCS facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) Owners or operators of OCS 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) The cognizant District Commander will examine each submission for compliance with this part and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

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

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

* * * * *

■ 18. In § 106.415, redesignate paragraph (a)(3) as paragraph (a)(4) and add new paragraph (a)(3) to read as follows:

§ 106.415 Amendment and audit.

(a) * * *

(3) Nothing in this section should be construed as limiting the OCS 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 District Commander 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.

* * * * *

Dated: October 8, 2003.

Thomas H. Collins,

Admiral, Coast Guard, Commandant.

[FR Doc. 03-26349 Filed 10-20-03; 8:45 am]

BILLING CODE 4910-15-U

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Parts 26, 161, 164, and 165

[USCG-2003-14757]

RIN 1625-AA67

Automatic Identification System; Vessel Carriage Requirement

AGENCY: Coast Guard, DHS.

ACTION: Final rule.

SUMMARY: This final rule adopts, with changes, the temporary interim rule that amends port and waterway regulations and implements the Automatic Identification System (AIS) carriage requirements of the Maritime Transportation Security Act of 2002 (MTSA) and the International Maritime Organization requirements adopted under International Convention for the Safety of Life at Sea, 1974, (SOLAS) as amended.

This rule is one in a series of final rules published 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-2003-14757 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>.

You may inspect the material incorporated by reference at room 1409, U.S. Coast Guard Headquarters, 2100 Second Street SW., Washington, DC 20593-0001 between 8:30 a.m. and 3:30 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-267-6277. Copies of the material are available as indicated in the "Incorporation by Reference" section of this preamble.

FOR FURTHER INFORMATION CONTACT: If you have questions on this final rule, call Mr. Jorge Arroyo, U.S. Coast Guard Office of Vessel Traffic Management (G-MWV), by telephone 202-267-6277, toll-free telephone 1-800-842-8740 ext. 7-6277, or electronic mail jarroyo@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 "Automatic Identification System; Vessel Carriage Requirement" in the **Federal Register** (68 FR 39353). 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 41913).

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 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 "Automated Identification System; Carriage Requirement" temporary interim rule. We have addressed individual comments in the preamble to the appropriate final rule. Additionally, we had several commenters submit the same comment to all six dockets. We counted these duplicate submissions as only one letter, and we addressed each comment within that letter in the preamble for the appropriate final rule. Because of statutorily imposed time constraints for publishing these regulations, we were unable to consider, in this Final Rule, comments received after the period for receipt of comments closed on July 31, 2003. Copies of late-received comments on AIS will be placed into the docket for the separate AIS Notice and request for comments that was published on July 1, 2003 (USCG 2003-14878; 68 FR 39369).

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. A transcript of this meeting is available in the docket, where indicated under **ADDRESSES**.

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. We will place a copy of the unofficial complete regulatory text in

the docket, where indicated under **ADDRESSES**.

Public Meetings for Rulemakings Related to Vessel Traffic Service

The Coast Guard held a public meeting on October 28, 1998, in New Orleans, Louisiana. The meeting was announced in a notice published in the **Federal Register** on September 18, 1998 (63 FR 49939). This meeting gave the Coast Guard the opportunity to discuss the Vessel Traffic Service (VTS) concept on the Lower Mississippi River and the envisioned use of automatic identification system technology in the VTS. At this 1998 meeting, we reported the preliminary results of tests conducted on the Lower Mississippi River using precursor AIS. The proposed VTS on the Lower Mississippi River is not discussed in this rulemaking because it is the subject of a separate rulemaking titled "Vessel Traffic Service Lower Mississippi River" (65 FR 24616, April 26, 2000; docket [USCG-1998-4399]). We copied those comments regarding AIS that were submitted to the VTS Lower Mississippi River docket and placed those copies in the docket for this final rule for historical purposes. However, most of those comments were not addressed in the preamble discussion of the temporary interim rule because they were no longer applicable or because they addressed a previous version of AIS and not the version required by this final rule.

Over the past few years, the Coast Guard has made AIS presentations at various public forums including Federal advisory committee meetings (Towing Safety Advisory Committee, National Offshore Safety Advisory Committee, Houston-Galveston Navigation Safety Advisory Committee and Navigation Safety Advisory Council). Moreover, the AIS-based Ports and Waterways Safety System project being installed at the VTS Lower Mississippi River is regularly discussed at the Lower Mississippi River Waterway Safety Advisory Committee meetings.

The Houston-Galveston Navigation Safety Advisory Committee and Lower Mississippi River Waterway Safety Advisory Committee are federally chartered advisory committees charged with making recommendations to the Coast Guard on matters relating to the safe and efficient transit of vessels on their respective waterways. These open forums have afforded the public, particularly those in the Gulf of Mexico and Mississippi River areas, the opportunity to comment on both VTS Lower Mississippi River and AIS issues.

The public's input was taken into account throughout this final rule.

Background and Purpose

Section 5004 of the Oil Pollution Act of 1990, as codified in 33 U.S.C. 2734, directed the Coast Guard to operate additional equipment, as necessary, to provide surveillance of tank vessels transiting Prince William Sound, Alaska. We have done so since 1994 through a system then known as "Automated Dependent Surveillance." Advances have taken place with this technology, now referred to as AIS. Section 102 of the Maritime Transportation Security Act of 2002 (MTSA) mandates that AIS be installed and operating on most commercial and passenger vessels on all navigable waters of the United States.

The version of AIS required by this final rule automatically broadcasts vessel and voyage-related information that is received by other AIS-equipped ships and shore stations. In the ship-to-shore mode, AIS enhances maritime domain awareness and allows for the efficient exchange of vessel traffic information that previously was only available via voice communications with a VTS. In ship-to-ship mode, an AIS provides essential information to other vessels, such as name, position, course, and speed that is not otherwise readily available on board vessels. In either mode, an AIS enhances the mariner's situational awareness, makes possible the accurate exchange of navigational information, mitigates the risk of collision through reliable passing arrangements, and facilitates vessel traffic management, while simultaneously reducing voice radiotelephone transmissions.

AIS has achieved acceptance through worldwide adoption of performance and technical standards developed to ensure commonality, universality, and interoperability. These recommendations have now been established and adopted as standards by the following diverse international bodies: The International Maritime Organization (IMO), the International Telecommunications Union (ITU), and the International Electrotechnical Commission (IEC). Further, installation of such equipment is required on vessels subject to the International Convention for the Safety of Life at Sea, 1974, (SOLAS), as amended.

The "Automatic Identification System; Vessel Carriage Requirement" temporary interim rule provides a comprehensive discussion on the applicability and compliance dates, AIS testing, the need for standardization, existing AIS-like systems, and the ports

and waterways safety system. This information will not be duplicated in this final rule, but remains available at the **Federal Register** (68 FR 39353) and in the docket for this rule (USCG-2003-14757).

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. 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.

General

One commenter requested that we extend the compliance date for passenger and fishing vessels to December 31, 2005, to take advantage of prospective, potentially lower cost, AIS devices.

We believe the costs of AIS will continue to decrease as more manufacturers, models and types are brought to market. We also welcome all efforts of international standards bodies and manufacturers, to date, to design and produce cost-effective AIS equipment. As these improved or less costly devices are submitted for type approval, the Coast Guard will decide whether they meet our requirements and the intent of the MTSA, and if need be, we will amend this rule accordingly to permit their use.

Twenty-one commenters stated various reasons why they opposed a carriage requirement for AIS. Three commenters stated that AIS would not provide increased security to vessels or ports, arguing that knowing the location of larger, slower vessels does not eliminate any threat and that smaller, more agile recreational vessels are more accessible to terrorists. Seven commenters stated that AIS has very limited security benefits, is technically limited due to its line-of-sight range, and to the extent it does work, it works equally well for governmental authorities and those who choose to do harm. Four commenters stated that AIS installation will not provide vessel operators with information on the identity of other commercial craft that is

not already available through basic visual or radio means. Three commenters stated that VTS areas would not receive information on non-applicable vessels that could pose threats. Eight commenters stated that the estimated cost would be a burden that most companies would be unable to bear. One commenter stated that the installation would distract the captain's attention from surrounding non-commercial recreational traffic and will clutter the pilothouse. One commenter stated that AIS is an outdated technology.

We acknowledge these limitations; however, we believe that AIS has the potential to mitigate collisions and the risk of a transportation security incident, as defined in the MTSA. We recognize that a single sensor, such as AIS, will not likely prevent a transportation security incident alone, but if AIS can have a mitigating effect on just a single collision or transportation security incident, the security benefit could be significant. Furthermore, under the MTSA, the Coast Guard is required to implement AIS carriage.

One commenter stated that costs for annual repairs and for the replacement of the AIS unit need to be calculated.

The Regulatory Assessment and Initial Regulatory Flexibility Act Analysis, available in the docket for this rule (USCG-2003-14757), included detailed estimates for annual repairs and periodic replacement. The summary included in the temporary interim rule reflects these costs.

One commenter believes it is inappropriate to analyze the economic impact of the cost using the "percentage of annual revenue that is first-year AIS cost," stating that it would be more appropriate to analyze the impact of the cost as a percentage of the net revenue of small businesses.

We recognize that using net revenues to determine the cost of this rule to small businesses would provide a more accurate picture of the effects of this rule on those entities, however this information is not available to the public. Thus, we used the information that is publicly available, the percentage of annual revenue, to analyze the economic impact of the cost of implementation on small businesses.

One commenter stated that our regulatory analysis is unclear as to whether the benefit assessment for AIS accounts for domestic vessels operating in VTS areas only, or applies to the entire inland waterway system.

In order to quantify the benefits of AIS implementation, the Coast Guard reviewed Marine Casualty Incident

Reports from 1993-1999 that involved the vessel populations affected by the temporary interim rule. This included domestic vessels operating in VTS areas, not the entire inland waterway system.

One commenter agreed with our economic analysis regarding AIS and with our assessment that the cost of AIS installation for the domestic fleet far outweighs the benefit.

While monetized safety benefits produced a low benefit-cost ratio, Congress mandated an AIS carriage requirement that included domestic vessels in 46 U.S.C. 70114 of the MTSA. In addition, we believe that AIS is critical to maritime domain awareness and, although our assessment could not quantify or monetize the benefits of the security contribution of AIS, we believe it has the potential to mitigate the consequences of a transportation security incident as described in the MTSA.

Nine commenters noted that AIS is duplicative of existing systems because fishing vessels are currently equipped with Vessel Monitoring System (VMS), which already fulfills the AIS monitoring aspect. Two commenters requested that existing satellite tracking systems, such as the VMS used by the National Marine Fisheries Service (NMFS) be allowed as an alternative to the AIS requirement.

As discussed in the "Existing AIS-Like Systems" section of the preamble to the temporary interim rule, there are many precursor and competing tracking systems in use today, VMS is just one of them. VMS is a system required by the NMFS as a means to monitor and enforce compliance with NMFS requirements. VMS relies upon International Mobile Satellite Organization (INMARSAT C) communication service providers to schedule or poll, one-way, traffic reports from the vessel to NMFS. AIS, conversely, is an open, two-way, non-proprietary system that is autonomous and self-organizing, requiring no shoreside commands for its operations. AIS is also a short-range VHF-FM system that provides a vessel's location more frequently than VMS. This permits AIS to be both a safety and security tool. Furthermore, AIS is not limited to one-way communications or tied to proprietary software or communications services, and AIS signals can be monitored from shore and from other vessels to provide greater maritime domain awareness.

One commenter recommended that we rewrite the final rule in plain language so that vessel owners and operators can easily understand the

carriage requirements and technical specifications.

We have attempted to make these final regulations as clear as possible. However, using plain language would require a complete rewrite of 33 CFR parts 26, 161, 164, and 165, which is beyond the scope of this rule.

Two commenters requested that the Coast Guard allow industry alternative programs as provided for in both facility and vessel security rules.

We are unable, at this time, to approve industry alternative programs for AIS. We do believe that it is a subject worthy of consideration, and welcome comments and suggestions on potential alternative programs for the AIS carriage requirement. We have published in the **Federal Register** (68 FR 55643) a notice reopening the comment period on our previously published notice titled "Automatic Identification System; Expansion of Carriage Requirements for U.S. Waters" (USCG 2003-14878; July 1, 2003; 68 FR 39369). Please send your comments on the use of an alternative program to that docket.

One commenter stated that the AIS regulation represents an unfunded mandate, stating that further discussion of funding for AIS purchase and maintenance is needed because vessel owners should not be expected to fund this.

As stated in the temporary interim rule and below, this final rule is exempted from assessing the effects of the regulatory action as required by the Unfunded Mandate Reform Act because it is necessary for the national security of the United States (2 U.S.C. 1503(5)). We are aware of the burden this rule places on industry. In order to re-evaluate this burden, we have amended the applicability section for this final rule (discussed below), and will reopen the comment period on our previously published notice titled "Automatic Identification System; Expansion of Carriage Requirements for U.S. Waters" (USCG 2003-14878; July 1, 2003; 68 FR 39369).

One commenter stated that vessels carrying AIS equipment should be released from liability whenever they are involved in a collision with a vessel that is not carrying AIS equipment.

While we appreciate the points raised concerning potential liability, the issue of liability is beyond the scope of this rule. No provision of the MTSA addresses liability, either to expressly limit liability or to address immunity from liability. Determinations of liability require a fact-laden inquiry on a case-by-case basis, and typically require complex analyses regarding matters such as choice of law, contracts,

and international conventions. Additionally, we note that carrying AIS does not relieve mariners from following all applicable navigation rules, and therefore may not be enough reason to relieve vessel owners and operators of liability.

Applicability

Five commenters supported our approach to AIS implementation. Three commenters expressed enthusiastic support for the AIS system, and agreed with the time schedule and criteria for SOLAS and domestic AIS carriage. Two commenters supported the decision to phase-in the requirements of the AIS regulation, and supported implementing the AIS requirements as a security measure, rather than as a safety tool.

One commenter asked whether U.S. government research ships are required to have AIS installed. If yes, the commenter asked what the time frame required for this installation is. Another commenter asked whether law enforcement and military vessels will carry AIS.

Sections 164.01(c) and 164.46(a)(1) were amended or added by the temporary interim rule (68 FR 39367) and state that the rules do not apply to government or non-commercial vessels. Therefore, these regulations do not apply to military, government, or public vessels so long as they are not used commercially. We do, however, encourage these vessels to voluntarily use AIS, as operational conditions may warrant, as will the Coast Guard fleet.

One commenter requested that the implementation date for AIS in the St. Mary's River Vessel Traffic Service (VTS) area be changed to January 31, 2005, from December 31, 2003, as published in the temporary interim rule, arguing that the December 31, 2003, implementation date is impractical based on vessel operations in the locks.

We agree that having the implementation deadline towards the end of a limited shipping season is impractical, but we do not agree with changing the date to January 31, 2005, because that date is beyond the deadline date established by the MTSA. In response, we have amended 33 CFR 164.46(a)(3) to apply uniformly to all VTS areas by December 31, 2004. We have made conforming amendments to §§ 164.43 and 165.1704 to reflect this change.

We received 47 comments requesting changes to the applicability of the AIS carriage requirement. Two commenters requested that passenger vessels be exempt from this rule. Two commenters asked why AIS is being required on vessels 65 feet and over. Four

commenters disagreed in general with the applicability of the AIS rule. Two commenters asked the Coast Guard to suspend the AIS requirements for the domestic fleet. Two commenters asked that we exempt commercial marine assistance vessels that operate in a limited geographical area. One commenter requested that we exempt sailing vessels from the AIS requirement. One commenter suggested that we exempt charter boats. Eleven commenters requested that fishing vessels also be exempt from or be given a waiver from this rule, citing high costs and minimal benefits. Eight commenters urged the Coast Guard to amend the AIS carriage requirement to apply to passenger vessels carrying more than 150 passengers, not 50 passengers, stating that this would ease the regulatory burden for the most economically vulnerable companies, improve the cost-benefit ratio for the domestic fleet, and align with the applicability requirements in 33 CFR subchapter H. Ten commenters asked whether the requirements for AIS carriage apply if a vessel spends periods of reduced operations in a VTS area but conducts commercial operations only outside the VTS. One of these commenters further added that the AIS requirement could impose unintended consequences on VTS ports and shipyards because owners may now decide to moor their vessels to non-VTS areas.

Congress mandated an AIS carriage requirement on commercial vessels over 65-feet in length in 46 U.S.C. 70114, and provided explicit deadlines for AIS in the MTSA, § 102(e). Under the MTSA, the Coast Guard is granted discretion as to which passenger vessels should be required to have AIS. In crafting the temporary interim rule, the Coast Guard took into consideration that Vessel Bridge-to-Bridge Radiotelephone and Vessel Movement Reporting System (VMRS) requirements apply to passenger vessels over 100 gross tonnage and those certificated to carry 50 passengers, and that this population comprises a large segment of VTS users. We believe that AIS is a key component in providing safety and security in VTS and VMRS areas and should cover as many vessels as practicable, including smaller passenger vessels. Nevertheless, the Coast Guard is removing the AIS carriage requirement for commercial fishing vessels and small passenger vessels certificated to carry less than 151 passengers. The Coast Guard is amending § 164.46(a)(3) accordingly and will reengage the public with respect to applicability and carriage requirements

for small passenger vessels and commercial fishing vessels.

To that end, the Coast Guard published in the **Federal Register** (68 FR 55643) a notice that reopened the comment period on our previously published notice titled "Automatic Identification System; Expansion of Carriage Requirements for U.S. Waters" (USCG 2003-14878; July 1, 2003; 68 FR 39369). The notice reopening the comment period included additional questions regarding expanding AIS carriage to small passenger vessels, whether infrequent VTS users (*e.g.*, fishing vessels) should be exempt from the AIS requirement, and whether exemptions may be granted by the VTS as a deviation request, as opposed to the written notification required in 33 CFR 164.55. By this action, we hope to generate further comments, discussion, and contributions from prospective mandatory users of AIS that we will then consider as we continue forward with future AIS rulemakings.

Five commenters stated that the AIS carriage requirement should be universal, arguing that an AIS carriage requirement that does not apply to every vessel, including recreational vessels, is of limited value as either a security or a safety tool.

We agree that AIS would provide the greatest benefit if all vessels were required to be equipped with an AIS unit. However, as with any new technology, AIS carriage must be implemented prudently. Therefore, the Coast Guard has chosen to implement AIS domestically beginning in VTS areas (as denoted in table 161.12(c), and will consider expanding AIS carriage to other waterways in consideration of comments received on our previously published notice titled "Automatic Identification System; Expansion of Carriage Requirements for U.S. Waters" (USCG 2003-14878; July 1, 2003; 68 FR 39369). Additionally, the AIS carriage requirements found in the MTSA do not apply to recreational vessels.

Upon further review, we have amended § 164.02 to clarify applicability for foreign vessels.

Technical

One commenter supported the AIS unit standardization proposal presented in the temporary interim rule.

One commenter asked if vessels that use an electronic chart to display AIS targets must have the chart updated and corrected to the latest Broadcast Notice to Mariners. The same commenter also asked if a vessel would still have to carry nautical charts if it uses an Electronic Chart Display and

Information System (ECDIS) to display AIS targets.

Mariners are advised that U.S. regulations or SOLAS requirements have always called for paper charts that are relied upon for the navigation of the vessel to be correct and up to date, regardless of whether they have AIS or can view vessels on an electronic chart.

One commenter expressed concerns over the electronic display of AIS data, stating that the technical limitations of commercial radar or ECDIS to merge data from the AIS is an issue.

We acknowledge the concerns expressed by the commenter. There are no international standards, at this time, for a manufacturer to rely upon to assure AIS buyers that an AIS may be properly integrated into other display devices. All AIS units come with a display that allows the user to input AIS information (e.g., vessel identity, dimensions, navigation status, antenna location) and to access all information received from other units. AIS also has multiple output options that facilitate using or integrating AIS data on other navigational systems, such as radar, Advanced Radar Plotting Aid (ARPA), ECDIS, and electronic charts. We have purposely not required this integration, or chosen a one-size fits all approach to graphical displays, in order to leave the choice with the mariner, who is best positioned to decide which output option suits the mariner's vessel and operation. Additionally, we are working diligently on this matter, commissioning the Transportation Research Board to develop recommendations for us, and working with various standards bodies to develop guidelines and standards.

One commenter stated that the IMO guidelines on installation of AIS devices might not be well suited for smaller vessels.

We agree; the IMO Installation Guidelines (particularly regarding antenna placement) are not well suited for smaller vessels. We will develop further guidelines to assist these vessel owners and operators with the installation of their AIS, and will place a copy in the docket and post a copy on our website at http://www.navcen.uscg.gov/enav/ais/AIS_carriage_reqmts.htm as soon as we have completed these guidelines.

One commenter asked whether AIS would require a backup power source.

Given the importance and value of AIS data to possible search and rescue efforts, we have begun work with IMO to require back-up power requirements, similar to those imposed on Global Maritime Distress and Safety System (GMDSS) equipment. Should these requirements be adopted by IMO, we

will propose regulatory amendments in a separate rulemaking to do the same for those vessels subject to SOLAS and strongly encourage the same on other vessels that transit the high seas.

Five commenters asked the Coast Guard to consider its ability to develop and support the public infrastructure necessary to fully support AIS and the availability of the radio-frequency bandwidth, citing the Coast Guard's recent history with similar projects (e.g., GMDSS). Five commenters asked us to resolve questions involving frequency allocation, stating that vessel operators should not be required to keep track of different frequency requirements and manually adjust their AIS units for each VTS area. Three commenters stated that it is up to the Coast Guard, not the FCC, to ensure that frequencies are available for AIS use.

We have considered our ability to develop and support the public infrastructure necessary to fully support AIS. We have chosen to require carriage of AIS in those areas that are being upgraded through our Ports and Waterways Safety System acquisition program. The Coast Guard does not have the authority to designate frequencies for AIS use, therefore, we requested and received frequency authorizations from the Federal Communication Commission (FCC) and the National Telecommunication and Information Agency (NTIA). Pending a rulemaking by FCC, we rely on the FCC decision stated in FCC Notice DA-02-1362 that states that the Commission "will consider the use of shipborne AIS equipment to be authorized by existing ship station licenses, including vessels that are licensed by rule." We agree that the operation of AIS should be seamless to the user, who should not be required to manually adjust their AIS units for each VTS area. FCC policies currently authorize the use of AIS frequencies (AIS1, Channel 87B, 161.975 MHz and AIS2, Channel 88B, 162.025 MHz) on existing ship station licenses. Should AIS frequency management be required due to the unavailability of AIS1 or AIS2 in any one VTS area, we intend to have the infrastructure in place to perform frequency management through the base station capabilities of AIS.

Five commenters stated that interference to adjacent channels would potentially result in the loss of property and life at sea.

AIS devices must fully comply with ITU and IEC standards and undergo an additional level of review not applicable to most other FCC type certified devices prior to being authorized to operate in the VHF marine band. Further, IMO has developed detailed guidelines (IMO SN/

Circ. 227) to be followed regarding the installation of AIS. These guidelines have been incorporated by reference into this regulation, as a requirement, in 33 CFR 164.03 and 164.46.

Notwithstanding this requirement, as is the case with any radiating or receiving radio device, there is always a possibility for radio interference when numerous emission devices are operating in the near vicinity of each other, particularly in a congested and noisy environment as exists on the VHF FM maritime band. The Coast Guard will be diligent in monitoring AIS use for interferences and will promptly mitigate them by enforcing the required installation guidelines, through the AIS type approval process, and through frequency plan coordination with existing public coast station licensees.

One commenter noted that the interference to adjacent channels from the currently adopted AIS carriage requirement is an unconstitutional taking of private property without just compensation.

The Coast Guard does not believe the MTSA or these regulations effect a taking, *inter alia*, because these regulations rely on FCC decisions to authorize existing shipboard licensees to operate AIS on the AIS frequencies. See FCC Public Notice DA-02-1622 (June 13, 2002). Additionally, we do not believe that the commenter's license constitutes a sufficient property interest to justify its position that this regulation constitutes a "taking." Finally, even assuming, without admitting that there is a legally cognizable property interest in the commenter's license, this regulation does not create such an interference with the commenter's use of that license as to constitute a regulatory taking in violation of the Constitution.

One commenter asked whether a fleet manager could buy an AIS base station to assist with the company dispatch and logistics.

Shoreside AIS stations, mistakenly referred to by some as AIS base stations, are subject to FCC regulation and licensing. FCC Notice DA-02-1362 permits the use of AIS by ship station licenses but did not address its similar use by VHF shore stations. Shoreside AIS stations enhance the AIS network because they control matters regarding frequency management, power setting, and allocation of AIS data slots, which are all functions that will be performed by the Coast Guard or another government entity.

Three commenters stated that the utility of AIS is considerably diminished if the system, as installed, is not capable of relaying information from

an automatic position indicating system and gyrocompass.

We recognize that the information provided by external sensors, such as a transmitting heading device, speed log, or navigation lights, to an AIS in accordance with the standards incorporated by reference in this regulation will provide the additional benefit to the user, as would integrating AIS with the existing on board navigation equipment. However, this integration technology and its accompanying standards are still being developed, thus, we did not require them. Each U.S. type approved AIS has a timing and positioning component built-in (*e.g.*, Global Positioning System) and the lack of additional sensor input does not diminish the utility of the AIS in providing for security and navigational safety.

One commenter asked whether AIS is an electronic aid to navigation as that term is used in 33 CFR 66.01-1, which states: "With the exception of radar beacons (racons) and shore-based radar stations, operation of electronic aids to navigation as private aids will not be authorized."

AIS is a navigational aid, but not necessarily an aid to navigation, as that term is used in 33 CFR part 66. In addition to increasing maritime domain awareness for security purposes, shipborne AIS is intended for collision avoidance, and not intended to be relied upon or referred to, as a buoy, lighthouse, or racon would be. AIS standards allow for the creation of AIS aids to navigation, and should we choose to use these aids, they will be catalogued in the Coast Guard's Light List as all other aids to navigation currently are.

One commenter stated that the Coast Guard must resolve questions over patent rights for the AIS standard prior to implementing a domestic carriage requirement.

Prospective AIS users should not be concerned with any patent issues regarding AIS or any other shipboard equipment. These are matters that need only be worked out by manufacturers of the devices and any patent holders.

One commenter asked whether vessels would be required to provide a Maritime Mobile Service Identifier (MMSI) and Universal Time Coordinated (UTC), stating that not all vessels currently have an MMSI. This commenter also asked how a vessel operator can be confident that the target identified on an AIS is who it says it is, if AIS units can be purchased from any commercial source, and an MMSI obtained from an FCC agent.

One goal of AIS is to lessen the reporting required by mariners. However, certain information and data input is necessary for the proper operation of an AIS. Many of these data fields are inputted only once, such as the vessel's identity, MMSI, dimensions, and antenna location. MMSI and UTC are critical to AIS; the MMSI (defined in note 1 to Table 161.12(c) of 33 CFR 161.12), which we have amended for clarity, provides a unique identifier for each AIS user, and the UTC is relied upon by the system to properly manage the AIS data link and network. UTC is provided internally by the AIS unit, and requires no input by the user. MMSI does need to be entered by the user, and is noted on the ship's station radio license issued by the FCC. Because user error is always possible, we urge users to be vigilant and request that you notify the nearest COTP if you encounter improper AIS usage.

Operations

One commenter recommended rewording § 164.46(a) because as presently drafted it could be incorrectly interpreted to mean that manufacturer self-certification of equipment to the listed standards would be sufficient.

We agree and have amended § 164.46(a) to require "type approved AIS."

One commenter stated that AIS is unnecessary because collision avoidance is best accomplished with an alert watch that is monitoring VHF channels, radar, GPS chart plotters, and depth sounders. This commenter stated that these technologies are already found on fishing vessels and it is not apparent that the addition of AIS will result in any significant benefit over maintaining a good watch.

We agree that competent and attentive watchkeeping is paramount to prudent navigation. We further note that prudent mariners are required to use all means available to avoid a collision. AIS is the latest navigation system to assist watchkeepers in the performance of their duties. None of the existing technologies found on commercial fishing vessels can accurately identify other vessels to the extent that AIS can. Additionally, in our analysis of costs and benefits, we found examples of marine casualties involving commercial fishing vessels that could have been prevented or mitigated with the use of AIS. More details on these casualties can be found in the Regulatory Assessment and Initial Regulatory Flexibility Act Analysis located in the docket for this rule (USCG-2003-14757).

One commenter asked us several questions regarding whether use of an AIS would satisfy various "Rules of the Road" under the International Regulations for Preventing Collisions at Sea (COLREGS) or the Inland Navigation Rules (33 U.S.C. 2000 and 1201, *et seq.*), such as the requirement for a lookout, the provision regarding safe speed, provisions regarding risk of collision, and coordinating passing arrangements.

AIS is the latest of the available means a mariner will have to prevent collisions at sea. It is not intended to replace any of the existing means commonly and traditionally used by mariners to ascertain the risk of collision such as radar, Automatic Radar Plotting Aids (ARPA), lookouts, binoculars, visual bearings, relative position maneuvering boards, and EDCIS, but it can certainly supplement them. AIS provides mariners with near real-time information regarding another vessel's identity, dimensions, speed over ground, course over ground, navigation status, and heading. It will aid mariners in identifying other vessels in restricted visibility, and those that would be indistinguishable in radar sea clutter. It displays the bearing and range of other AIS-equipped vessels and provides another means of reliable communication by using ship-to-ship addressed text messages. In the future VTSs will be able to relay information on vessels not carrying AIS to AIS users. However, AIS should not be relied upon as the sole means to determine risk of collision, safe speed, or to avoid collision.

In the temporary interim rule, we discussed that AIS can assist mariners in coordinating passing arrangements. AIS will allow mariners to accurately identify a vessel by name and call sign to effectively make passing arrangements, thus replacing vague radio calls such as "vessel off my port bow" with more descriptive calls such as "vessel NAME/Call sign, bearing XXX degrees and XX meters." While AIS allows for ship-to-ship text messaging to communicate with others and make passing arrangements, these private communications do not meet the requirements of the Vessel Bridge-to-Bridge Radiotelephone Act (33 U.S.C. 1201 *et seq.*) for open broadcasts on the designated bridge-to-bridge channel, nor does it relieve a vessel operator from the requirement to sound whistle signals.

Three commenters asked the Coast Guard to test AIS on vessels on the Lower Mississippi River, stating that previous tests were not adequate.

We do not believe that additional testing on the Lower Mississippi River

is necessary prior to implementation. The Coast Guard conducted exhaustive testing of precursor AIS in cooperation with stakeholders on the Lower Mississippi River. We detailed this testing in the "AIS Testing" section of the preamble to the AIS temporary interim rule (68 FR 39357). We also conducted tests with the AIS being required in this regulation (ITU-R M.1371-1) in other VTS areas, and monitored similar tests conducted in other countries. However, the Coast Guard will continue to conduct system acceptance testing of the newly installed AIS shoreside network in the Lower Mississippi River.

Five commenters stated that AIS should require only minimal information from vessel operators, so that the information flow to and from AIS does not distract vessel operators from their other duties.

We agree that AIS users should not be burdened unnecessarily. One goal of AIS is to unburden mariners from the important, although tedious, tasks of reporting information to a VTS. Through AIS these reports are automated and additional voyage data may be transmitted. Whether vessels are required to supply this additional data (people on board, destination, and estimated time of arrival) will be determined by the VTS, which will take into consideration the reporting exemptions listed in 33 CFR 161.23.

One commenter asked whether the operator of a vessel entering a VMRS area must call the VTS on a VHF voice channel and whether the VTS will notify users of required actions by message or on VHF voice channels.

This rule mandates AIS position reports in lieu of VTS voice reports; however, it does not abolish the requirements set forth in 33 CFR part 161 regarding deviation requests, monitoring requirements, sailing plans, and final reports. Additionally, VTS and VTS users should still rely upon VHF voice communications on the designated VTS frequencies as the primary mode of VTS communication. VTS areas will eventually supplement these broadcasts with pertinent AIS text or binary messages.

One commenter asked whether a vessel could use AIS as a tool even if the vessel is communicating with is not in sight, citing confusion with the COLREGS and Inland Navigation Rules Eleven to Eighteen.

Inland Navigation Rule Three clearly states that vessels are deemed to be in sight of one another only when one can be observed visually from the other, not when observed electronically (e.g., AIS or radar). However, AIS-like radar—is

still a useful tool to use when making navigational decisions prior to being in the sight of another vessel.

One commenter asked for clarification on the training requirements for an AIS operator.

At this time, we envision no additional training requirements other than reading the AIS owner's manual and being familiar with operation of the AIS. However, mariners seeking a greater understanding of AIS and its uses may wish to read a document developed by the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) titled "IALA Guidelines on the Universal Automatic Identification System (AIS), Volume 1, Part 1—Operational Issues, Edition 1.1, December 2002," that is available at <http://www.iala-aism.org>.

One commenter asked how many vessels are displayed on an AIS when a vessel is in a crowded harbor.

AIS is designed to provide information on a minimum of the 20 closest active AIS targets.

Editorial

The temporary interim rule contained a typographical error, which is corrected in this rule. In §§ 164.03 and 164.46, the IMO circular "Guidelines for Installation of Shipborne Automatic Identification System (AIS), dated January 6, 2003" should have been titled "SN/Circ.227" vice "SN/Circ.277."

We have also added a note to 33 CFR 164.46(a) to clarify which international tonnage convention is being identified.

Procedural

Five commenters requested a longer comment period specifically for the AIS temporary interim rule.

We did not extend the comment period on this rule due to the need to follow the MTSA's statutory deadline for issuance of regulations. We acknowledge that these regulations are being implemented in a short period of time. We have, however, reopened the comment period on our previously published notice titled "Automatic Identification System; Expansion of Carriage Requirements for U.S. Waters" (USCG 2003-14878; July 1, 2003; 68 FR 39369).

Incorporation by Reference

The Director of the Federal Register has approved the material in § 164.03 for incorporation by reference under 5 U.S.C. 552 and 1 CFR part 51. You may inspect this material at U.S. Coast Guard Headquarters where indicated under **ADDRESSES**. Copies of the material are

available from the sources listed in § 164.03.

Regulatory Assessment

This final rule is a "significant regulatory action" under section 3(f) of Executive Order 12866, Regulatory Planning and Review. The Office of Management and Budget has reviewed it under that Order. It requires an assessment of potential costs and benefits under section 6(a)(3) of that Order. It is significant under the regulatory policies and procedures of the Department of Homeland Security. A final assessment is available in the docket as indicated under **ADDRESSES**. A summary of the assessment and changes from the draft assessment follows.

Cost Assessment

This final rule is requiring the carriage of AIS on all U.S. flag SOLAS vessels, certain domestic vessels in VTS areas, and foreign flag vessels less than 300 gross tonnage that call on ports in the U.S. We estimate that 438 U.S. flag SOLAS vessels, 2,963 non-SOLAS domestic vessels, and 70 non-SOLAS foreign vessels will be affected by this final rule.

The estimated total present value cost of this final rule is \$50.4 million (where the period of analysis is 2003-2012). An estimated present value \$5.2 million is for the U.S. flag SOLAS fleet, \$44.1 million is for the domestic, non-SOLAS fleet in VTS areas, and \$1.1 million is for the foreign, non-SOLAS fleet that call on ports in the U.S.

In the first year of implementation, the estimated cost is \$1.9 million for the U.S. flag SOLAS fleet, \$27.6 million for the domestic, non-SOLAS fleet in VTS areas, and less than \$1 million for the foreign, non-SOLAS fleet. Following initial implementation, the estimated annual cost is less than \$1 million for the entire affected population.

Safety Benefits

The Coast Guard expects both quantifiable and non-quantifiable benefits as a result of the final rule. Quantified benefits include avoided property damage, injuries, fatalities, and pollution events as a result of having an AIS. Other benefits include better situational awareness, information, and communications. The final rule will also enhance Coast Guard missions such as marine safety and security, aids to navigation, and maritime mobility.

In order to quantify the benefits of AIS implementation, the Coast Guard reviewed Marine Casualty Incident Reports (MCIRs) from 1993-1999 that involved the vessel populations affected by this final rule. These incidents were

used to develop a historical rate of marine casualties in VTS areas to determine the effectiveness of AIS as a mitigating factor.

The estimated total present value benefit of the final rule is \$24.4 million (2003–2012). An estimated present value \$13.3 million is for the U.S. flag SOLAS fleet, \$11.1 million is for the domestic, non-SOLAS fleet in VTS areas. We did not find any quantified safety benefits for the foreign, non-SOLAS fleet.

Security Benefits

This final rule is one of six final rules that implement national maritime security initiatives concerning general provisions, Area Maritime Security (ports), vessels, facilities, Outer Continental Shelf (OCS) facilities, and AIS. The Coast Guard used the National Risk Assessment Tool (N–RAT) to assess benefits that would result from

increased security for vessels, facilities, OCS facilities, and areas. The N–RAT considers threat, vulnerability, and consequences for several maritime entities in various security-related scenarios. For a more detailed discussion on the N–RAT and how we employed this tool, refer to “Applicability of National Maritime Security Initiatives” in the temporary interim rule titled “Implementation of National Maritime Security Initiatives” (68 FR 39243) (part 101). For this benefit assessment, the Coast Guard used a team to calculate a risk score for each entity and scenario before and after the implementation of required security measures. The difference in before and after scores indicated the benefit of the proposed action.

We recognized that the final rules are a “family” of rules that will reinforce and support one another in their implementation. We have ensured,

however, that risk reduction that is credited in one rule is not also credited in another. For a more detailed discussion on the benefit assessment and how we addressed the potential to double-count the risk reduced, refer to “Benefit Assessment” in the temporary interim rule titled “Implementation of National Maritime Security Initiatives” (68 FR 39274) (part 101).

We determined annual risk points reduced for each of the six final rules using the N–RAT. The benefits are apportioned among the vessel, facility, OCS facility, area, and AIS rules. As shown in Table 1, the implementation of AIS for the affected population reduces 1,422 risk points annually through 2012. The benefits attributable for part 101, General Provisions, were not considered separately since this part 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
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 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.

Although we have quantified these security benefits relative to AIS, the N–RAT is limited in its ability to measure benefits attributable to intelligence or information gathering. These limitations are discussed in the

“Assessment Limitations” section in the preamble of the temporary interim rule titled “Implementation of National Maritime Security Initiatives” (USCG–2003–14792).

Congress mandated an AIS carriage requirement on domestic (non-SOLAS) vessels in 46 U.S.C. 70114, and provided an explicit phase-in schedule for AIS in section 102(e) of the MTSA. Strictly upon consideration of

monetized safety benefits, as measured through decreased collisions and the resulting decrease in injuries, mortalities, and pollution incidents, the cost of AIS installation for the domestic fleet far outweighs the benefit over a 10-year period (0.25 benefit-cost ratio). This ratio results from the high costs of purchasing and installing the unit (an estimated \$9,330 per vessel), and the types of marine casualties that AIS is expected to mitigate, where damage is not usually severe nor is there significant loss of life. In view of the benefit-cost ratio presented above, the Coast Guard has shared with the Congress all significant information provided by the public that addresses the reasonableness of implementing the statute. A copy of this letter is available in the docket where indicated under **ADDRESSES**.

Because there is not yet a mass market for AIS, the cost per unit in the next few years, when the domestic fleet is required to purchase AIS, is likely to be higher than when it is replaced (around 2012). Because the AIS market is in its infancy, we cannot estimate how much the unit cost will decrease over the next decade. If many manufacturers enter the market, costs are likely to drop through competition. Because manufacturers have a potential world market and a significant U.S. market, many may attempt to capture a segment. Conversely, if only a few players emerge worldwide, AIS costs could remain high. Because manufacturers must engage in a rigorous approval process and cannot be assured that they will recoup research and development costs through unit sales, there is the potential that only a few dominant players will emerge in the AIS market. Because we cannot determine the trend of the AIS market and we did not want to understate the cost for AIS, we assumed that the cost for units in 2012 would again be approximately \$9,000 per unit. It is possible that an AIS unit will not be this expensive to replace.

In terms of security, we estimated that we will not experience a significant benefit from a decrease in risk, as measured in risk points reduced in the N-RAT, as a result of AIS installation. There are two primary reasons for this estimate. First, the N-RAT was an internal Coast Guard tool that was modified to estimate the national benefits attributable to the suite of security rules mandated by the MTSA. The tool was not designed to measure the security benefits of AIS specifically. The N-RAT does not, therefore, robustly capture the risk mitigation potential of AIS. Second, the Coast Guard strongly believes that AIS is critical to maritime

domain awareness. However, we are unable to quantify or monetize the benefits of this Coast Guard mission or the individual contribution of AIS to it.

While the monetized benefit of the rule does not exceed its cost, the Coast Guard believes that AIS has the potential to mitigate a transportation security incident. The Coast Guard recognizes that a single sensor, such as AIS, will not likely prevent a transportation security incident alone—but if AIS can have a mitigating effect on just a single incident, the security benefit could be significant. The Coast Guard must consider AIS in its suite of security rules and has developed a final rule that considers the mandates of the MTSA in light of the high initial costs of purchasing the unit by requiring AIS in VTS areas only for the domestic fleet. We are concentrating our efforts in VTS areas since this is where we can begin accruing the most benefit—for industry, the public, and the Coast Guard—in the shortest period of time. However in response to public comment, in § 164.46(a)(1) and (a)(2)(i), we have removed the carriage requirement of the temporary interim rule for commercial fishing vessels and some small passenger vessels. Through this final rule we are attempting to maximize the return on investment as quickly and as effectively as practical.

Small Entities

Under the Regulatory Flexibility Act (5 U.S.C. 601–612), we have considered whether this 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 rule on small entities is available in the docket where indicated under **ADDRESSES**.

Number and Types of Small Entities Affected

U.S. Flag SOLAS Vessels

Of the affected population, we estimated that of the 438 total U.S. flag SOLAS vessels, 205 are owned by 122 small businesses. The remaining 233 vessels are owned by approximately 40 large companies.

We estimated the cost of an AIS unit per vessel in the first year will be

\$9,330. Of this, \$7,000 is for the AIS unit, \$2,000 is for installation, and \$330 is for mariner training. We estimated that following installation, each AIS will require \$250 in annual maintenance to replace such items as the antenna, keyboard, and display screen. We estimated that the entire unit will be replaced after eight years.

We found that annual maintenance costs will have a less-than-1-percent impact on annual revenue for all small businesses with U.S. flag SOLAS vessels. First-year impacts to small businesses, therefore, are the focus of this analysis. To estimate the revenue impact on small businesses in the first year, the cost per vessel for AIS, \$9,330, was multiplied by the number of vessels owned by each company, then divided by the average annual revenue for each company, as reported in the online databases. Of the 122 small businesses that own U.S. flag SOLAS vessels, we found revenue for 59 of them (48 percent). Table 3 presents the revenue impact for the 59 entities with known average annual revenue.

TABLE 3.—EFFECT OF FIRST-YEAR COST ON AVERAGE ANNUAL REVENUE FOR SMALL ENTITIES OWNING U.S. FLAG SOLAS VESSELS

Percent of annual revenue that is first-year AIS cost	Number of entities with known annual revenues	Percent of entities with known annual revenues
0–3	43	73
> 3–5	5	8
> 5–10	4	7
> 10–20	6	10
> 20–30	0	0
> 30	1	2
Total	59	100

As shown, the final rule will have a less-than-3-percent impact on 73 percent of small businesses owning non-SOLAS vessels in the first year it is in effect. Approximately 88 percent have a less-than-10-percent impact.

Number and Types of Small Entities Affected: Non-SOLAS Fleet in VTS Areas

We estimated that there are 637 small businesses that will be affected by the final rule that own non-SOLAS vessels that transit VTS areas. These 637 companies own 1,349 vessels, representing 46 percent of the 2,963 non-SOLAS vessels affected by the rule. An estimated 1,456 vessels (49 percent) are owned by 150 large businesses, and 55 vessels (2 percent) are owned by State and local governments. There are

103 vessels that transit VTS areas (3 percent of the non-SOLAS fleet) that have no company associated with the vessel due to missing company information in our data. We could not be certain if these vessels belong to small, large, or government entities and did not apportion these 103 vessels to one type of entity or another.

We estimated the cost of AIS per vessel in the first year will be \$9,330. As with the U.S. flag SOLAS fleet, annual cost following installation of AIS will have little impact on annual revenues—a less-than-1 percent impact on annual revenue for most small businesses. The first-year cost of this final rule, therefore, will again have the greatest impact on average annual revenue. To estimate the revenue impact on small businesses in the first year, the cost per vessel for AIS, \$9,330, was multiplied by the number of vessels owned by each company, then divided by the average annual revenue for each company. Of the 637 small businesses that own non-SOLAS vessels in VTS areas, we found revenue for 392 of them (62 percent). The results of the analysis for the non-SOLAS fleet in VTS areas with known company information are presented in Table 4.

TABLE 4.—EFFECT OF FIRST-YEAR COST ON AVERAGE ANNUAL REVENUE FOR SMALL ENTITIES OWNING DOMESTIC, NON-SOLAS VESSELS IN VTS AREAS

Percent of annual revenue that is first-year AIS cost	Number of entities with known annual revenues	Percent of entities with known annual revenues
0–3	303	77
> 3–5	32	8
> 5–10	28	7
> 10–20	15	4
> 20–30	10	3
> 30	4	1
Total	392	100

As shown, the final rule will have a less-than-3-percent impact on 77 percent of small businesses owning non-SOLAS vessels in the first year it is in effect. Approximately 92 percent have a less-than-10-percent impact. We concluded, therefore, that this final rule may have a significant economic impact on a substantial number of small entities.

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). The reports required by this rule are considered to be operational communications, transitory in nature, and, do not constitute a collection of information under the Paperwork Reduction Act.

We did not receive comments regarding collection of information.

Federalism

A rule has implications for Federalism under Executive Order 13132, Federalism, if it has a substantial direct effect on State or local governments and would either preempt State law or impose a substantial direct cost of compliance on them. It is well settled that States may not regulate in categories reserved for regulation by the Coast Guard. It is also well settled, now, that all of the categories covered in 46 U.S.C. 3306, 3703, 7101, and 8101 (design, construction, alteration, repair, maintenance, operation, equipping, personnel qualification, and manning of vessels), as well as the reporting of casualties and any other category in which Congress intended the Coast Guard to be the sole source of a vessel’s

obligations, are within the field foreclosed from regulation by the States. In addition, under the authority of Title I of the Ports and Waterways Safety Act, 33 U.S.C. 1221–1232 (specifically 33 U.S.C. 1223) and the MTSA this regulation will preempt any State action on the subject of Automatic Identification System carriage requirements. (See the decision of the Supreme Court in the consolidated cases of *United States v. Locke* and *Intertanko v. Locke*, 529 U.S. 89, 120 S. Ct. 1135 (March 6, 2000).) Our AIS carriage requirement rule falls into the category of equipping of vessels. Because the States may not regulate within this category, preemption under Executive Order 13132 is not an issue.

We did not receive comments regarding Federalism.

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 1 year. We discuss the effects of this final rule elsewhere in this preamble. However, this final rule is exempted from assessing the effects of the regulatory action as required by the Act because it is necessary for the national security of the United States (2 U.S.C. 1503(5)).

We did receive one comment regarding the Unfunded Mandates Reform Act; this comment is discussed within the “Discussion of Comments and Changes” section of this preamble.

Taking of Private Property

This final rule will not effect a taking of private property or otherwise have taking implications under Executive Order 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights. We did receive one comment regarding the taking of private property; this comment is 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 enhanced maritime security, 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)(d), (34)(e), and (34)(i) of Commandant Instruction M16475.ID, this rule is categorically excluded from further environmental documentation. This final rule concerns vessel equipment requirements that will contribute to a higher level of marine safety and maritime domain awareness

for U.S. port and waterways. A "Categorical Exclusion Determination" is available in the docket where indicated under **ADDRESSES**.

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

We did not receive comments regarding the environment.

List of Subjects

33 CFR Part 26

Communications equipment, Marine safety, Radiotelephone, Vessels.

33 CFR Part 161

Harbors, Navigation (water), Reporting and recordkeeping requirements, Vessels, Waterways.

33 CFR Part 164

Incorporation by reference, Marine safety, Navigation (water), Reporting and recordkeeping requirements, Waterways.

33 CFR Part 165

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

Accordingly, the interim rule amending 33 CFR parts 26, 161, 164, and 165 that was published at 68 FR 39353 on July 1, 2003, and amended at 68 FR 41913 on July 16, 2003, is adopted as a final rule with the following changes:

PART 161—VESSEL TRAFFIC MANAGEMENT

■ 1. The authority citation for part 161 continues to read as follows:

Authority: 33 U.S.C. 1223, 1231; 46 U.S.C. 70114, 70117; Pub. L. 107-295, 116 Stat. 2064; Department of Homeland Security Delegation No. 0170.1.

§ 161.12 [Amended]

■ 2. In § 161.12, in note 1 following table 161.12(c), add the following sentence to the end of the note: "The requirements set forth in §§ 161.21 and 164.46 of this subchapter apply in those areas denoted with a MMSI number."

PART 164—NAVIGATION SAFETY REGULATIONS

■ 3. The authority citation for part 164 continues to read as follows:

Authority: 33 U.S.C. 1223, 1231; 46 U.S.C. 2103, 3703, 70114, 70117; Pub. L. 107-295,

116 Stat. 2064; Department of Homeland Security Delegation No. 0170.1. Sec. 164.13 also issued under 46 U.S.C. 8502. Sec. 164.61 also issued under 46 U.S.C. 6101.

■ 4. In § 164.02, revise paragraph (a) introductory text to read as follows:

§ 164.02 Applicability exception for foreign vessels.

(a) Except as provided in § 164.46(a)(2) of this part, including §§ 164.38 and 164.39, this part does not apply to vessels that:

* * * * *

§ 164.03 [Amended]

■ 5. In § 164.03(b), under "International Maritime Organization", remove the word "SN/Circ.277" and add, in its place, the word "SN/Circ.227".

§ 164.43 [Amended]

■ 6. In § 164.43, in paragraph (a) introductory text, remove the words "July 1" and add, in their place, the words "December 31".

■ 7. Revise § 164.46 to read as follows:

§ 164.46 Automatic Identification System (AIS).

(a) The following vessels must have a properly installed, operational, type approved AIS as of the date specified:

(1) Self-propelled vessels of 65 feet or more in length, other than passenger and fishing vessels, in commercial service and on an international voyage, not later than December 31, 2004.

(2) Notwithstanding paragraph (a)(1) of this section, the following, self-propelled vessels, that are on an international voyage must also comply with SOLAS, as amended, Chapter V, regulation 19.2.1.6, 19.2.4, and 19.2.3.5 or 19.2.5.1 as appropriate (Incorporated by reference, see § 164.03):

(i) Passenger vessels, of 150 gross tonnage or more, not later than July 1, 2003;

(ii) Tankers, regardless of tonnage, not later than the first safety survey for safety equipment on or after July 1, 2003;

(iii) Vessels, other than passenger vessels or tankers, of 50,000 gross tonnage or more, not later than July 1, 2004; and

(iv) Vessels, other than passenger vessels or tankers, of 300 gross tonnage or more but less than 50,000 gross tonnage, not later than the first safety survey for safety equipment on or after July 1, 2004, but no later than December 31, 2004.

(3) Notwithstanding paragraphs (a)(1) and (a)(2) of this section, the following vessels, when navigating an area denoted in table 161.12(c) of § 161.12 of this chapter, not later than December 31, 2004:

(i) Self-propelled vessels of 65 feet or more in length, other than fishing vessels and passenger vessels certificated to carry less than 151 passengers-for-hire, in commercial service;

(ii) Towing vessels of 26 feet or more in length and more than 600 horsepower, in commercial service;

(iii) Passenger vessels certificated to carry more than 150 passengers-for-hire.

Note to § 164.46(a): “Properly installed” refers to an installation using the guidelines set forth in IMO SN/Circ.227 (incorporated by reference, see § 164.03). Not all AIS units are able to broadcast position, course, and speed without the input of an external positioning device (e.g. dGPS); the use of other external devices (e.g. transmitting heading device, gyro, rate of turn indicator) is highly recommended, however, not required except as stated in § 164.46(a)(2). “Type approved” refers to an approval by an IMO recognized Administration as to comply with IMO Resolution

MSC.74(69), ITU-R Recommendation M.1371-1, and IEC 61993-2 (Incorporated by reference, see § 164.03). “Length” refers to “registered length” as defined in 46 CFR part 69. “Gross tonnage” refers to tonnage as defined under the International Convention on Tonnage Measurement of Ships, 1969.

(b) The requirements for Vessel Bridge-to-Bridge radiotelephones in §§ 26.04(a) and (c), 26.05, 26.06 and 26.07 of this chapter also apply to AIS. The term “effective operating condition” used in § 26.06 of this chapter includes accurate input and upkeep of AIS data fields.

(c) The use of a portable AIS is permissible only to the extent that electromagnetic interference does not affect the proper function of existing navigation and communication equipment on board and such that only one AIS unit may be in operation at any one time.

(d) The AIS Pilot Plug, on each vessel over 1,600 gross tons on an international

voyage, must be available for pilot use, easily accessible from the primary conning position of the vessel, and near a 120 Volt, AC power, 3-prong receptacle.

PART 165—REGULATED NAVIGATION AREAS AND LIMITED ACCESS AREAS

■ 8. The authority citation for part 165 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191, 195; 33 CFR 1.05-1(g), 6.04-1, 6.04-6, and 160.5; Pub. L. 107-295, 116 Stat. 2064; Department of Homeland Security Delegation No. 0170.1.

§ 165.1704 [Amended]

■ 9. In § 165.1704(c)(6), remove the words “July 1” and add, in their place, the words “December 31”.

Dated: October 8, 2003.

Thomas H. Collins,

Admiral, Coast Guard, Commandant.

[FR Doc. 03-26350 Filed 10-20-03; 8:45 am]

BILLING CODE 4910-15-U