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 Indentification 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 ''vitally important to the local economy, as well as to the host municipalities.'' This commenter also stated that vessels certificated to carry more than 150 passengers frequently embark guests at private, residential docks and small private marinas for special events such as weddings and anniversaries and may visit such a dock only once.

We agree that the applicability of part 105 to facilities that have minimal infrastructure, but are capable of receiving passenger vessels, is unclear. Therefore, 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 Alterative 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 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

[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/usfwts/.*

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

[4] *See* footnote 1.

[5] *See* footnote 1.

[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.

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.lD, 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 for ''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 TRANSPORATION 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