## DEPARTMENT OF HOMELAND SECURITY

## Coast Guard

## 33 CFR Part 106

**[USCG–2003–14759]**

**RIN 1625–AA68**

## Outer Continental Shelf Facility Security

**AGENCY:** Coast Guard, DHS.

**ACTION:** Final rule.

**SUMMARY:** This final rule adopts, with changes, the temporary interim rule published on July 1, 2003, that provides security measures for mobile offshore drilling units (MODUs) not subject to the International Convention for the Safety of Life at Sea, 1974, and certain fixed and floating facilities on the Outer Continental Shelf (OCS) other than deepwater ports. This rule also requires the owners or operators of OCS facilities to designate security officers for OCS facilities, develop security plans based on security assessments and surveys, implement security measures specific to the OCS facility's operation, and comply with Maritime Security Levels. This rule is one in a series of final rules on maritime security in today's **Federal Register**. To best understand this rule, first read the final rule titled ''Implementation of National Maritime Security Initiatives'' (USCG–2003–14792), published elsewhere in today's **Federal Register**.

**DATES:** This final rule is effective November 21, 2003. On July 1, 2003, the Director of the Federal Register approved the incorporation by reference of certain publications listed in this final rule.

**ADDRESSES:** Comments and material received from the public, as well as documents mentioned in this preamble as being available in the docket, are part of docket USCG–2003–14759 and are available for inspection or copying at the Docket Management Facility, U.S. Department of Transportation, room PL–401, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet at http://dms.dot.gov.

**FOR FURTHER INFORMATION CONTACT:** If you have questions on this final rule, call Lieutenant Greg Versaw (G–MPS–2), U.S. Coast Guard by telephone 202–267–4144 or by electronic mail *gversaw@comdt.uscg.mil.* If you have questions on viewing the docket, call Andrea M. Jenkins, Program Manager, Docket Operations, Department of Transportation, at telephone 202–366–0271.

**SUPPLEMENTARY INFORMATION:**

### Regulatory Information

On July 1, 2003, we published a temporary interim rule with request for comments and notice of public meeting titled ''Outer Continental Shelf Facility Security'' in the **Federal Register** (68 FR 39338). This temporary interim rule was one of a series of temporary interim rules on maritime security published in the July 1, 2003, issue of the **Federal Register**. On July 16, 2003, we published a document correcting typographical errors and omissions in that rule (68 FR 41916).

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

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

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

### Background and Purpose

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

### Discussion of Comments and Changes

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

*Subpart A—General*

This subpart contains provisions concerning applicability, waivers, and other subjects of a general nature applicable to part 106.

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

The purpose of the broad definition of ''OCS facility'' in § 101.105 is to ensure that OCS facilities that are not regulated under part 106 will be covered by parts 101 through 103. The proposed additional language would not add clarity to part 106 because the applicability in § 106.105 states that the section applies only to those MODUs that are operating for the purposes of engaging in the exploration, development, or production of oil, natural gas, or mineral resources.

Two commenters suggested amending the definition of ''owner or operator'' so

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

We disagree with adding the suggested language of the first commenter because we have concluded that the person with operational control is the best person to implement these regulations and, therefore, should be responsible for implementation. The language proposed would include a lessee regardless of whether or not that lessee maintains such operational control. We also disagree with adding the suggested language of the second comment because it would be unnecessarily limiting.

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

With regard to the definition of ''facility'' and the suggested additional language regarding MODUs, the definition clearly incorporates MODUs that are not covered under part 104 and MODUs that are sufficiently covered under parts 101 through 103 and 106. Therefore, we are not amending our definition of facility nor incorporating the suggested explicit exemption from part 105 because these MODUs are excluded. We have, however, amended the applicability section of part 104 (§ 104.105) so that foreign flag, non-self propelled MODUs that meet the threshold characteristics set for OCS facilities are regulated by 33 CFR part 106, rather than 33 CFR part 104. We have done so because MODUs act and function more like OCS facilities, have limited interface activities with foreign and U.S. ports, and their personnel undergo a higher level of scrutiny to obtain visas to work on the Outer Continental Shelf. These amendments to § 104.105 required us to add a definition for ''cargo vessel'' in § 101.105. With these changes, we believe the existing definitions of ''facility'' and ''OCS facility'' in § 101.105 are sufficient to conclusively identify those entities that are subject to parts 104, 105, and 106. In addition, the definition of ''OCS facility,'' as written, ensures that these entities will be subject to relevant elements of an OCS Area Maritime Security (AMS) Plan. We believe the language in § 106.105, read in concert with the amended § 104.105(a)(1), and the existing definitions in part 101, is sufficient to preclude MODUs that are in compliance with part 104 from being subject to part 106.

We received four comments on the applicability of part 106 to certain OCS facilities. Three commenters stated that the operating conditions referenced in § 106.105 should remain as written. A fourth commenter stated that the size criteria used in § 106.105 contains no support; that the regulations are a duplication of existing informal security measures; that the regulations do not define ''adequate level of security'' and offer no support that scrutiny of personnel and cargo will, or has in the past, prevented terrorist attacks; that the rule imposes a huge paperwork and formal reporting burden; that training of employees to detect dangerous situations and devices on facilities located more than 100 miles from shore is unreasonable; that the security provided by the Declaration of Security is minimal; that there is no need for the OCS Facility Security Assessment; and that the OCS Facility Security Plan will offer no security from exterior threats.

As discussed in the temporary interim rule titled ''Implementation of National Maritime Security Initiatives'' (68 FR 39250), we determined the applicability of part 106 for those facilities that may be involved in a transportation security incident. In developing part 106 and the security measures in it, we deliberately reviewed and incorporated much of the pre-existing informal security measures to ensure standardization and minimize the burden to those in industry that have already voluntarily adopted standards. We have determined that the security measures in part 106 will reduce the likelihood of a transportation security incident by increasing the awareness of security threats to the OCS facility. We believe that the best means of deterring incidents is to reduce the vulnerabilities of the OCS facility to a security threat by ensuring that the owner or operator of that OCS facility increases their vigilance, awareness, and control over the vessels and persons that interact with the OCS facility. The OCS Facility Security Assessment and Plan are not envisioned to be the sole means of deterrence against security incidents. All of the security plans of the National Maritime Security Initiatives work in conjunction to reduce the vulnerability of the Marine Transportation System from various types of attacks originating from air, land, and sea. We recognize that we impose a requirement for the submission of assessments and plans to ensure compliance. To reduce the overall paperwork burden, we allow a single plan to cover multiple OCS facilities.

After further review of § 106.105 and discussion with the Minerals Management Service (MMS), we have determined that there may be OCS facilities acting as ''hubs'' for oil transportation that do not meet the production characteristics that are regulated under this part. However, due to unique local conditions, specific intelligence information, or other identifiable and articulable risk factors, these ''hub'' facilities may be involved in a transportation security incident. Therefore, on a case-by-case basis, these ''hub'' facility operations will be reviewed and, if appropriate, a MARSEC Directive will be issued to address these circumstances.

One commenter asked how OCS facilities not directly regulated under part 106 would be regulated.

As indicated in § 103.100, all facilities located in waters subject to the jurisdiction of the U.S. are covered by part 103 and must comply with the requirements in the AMS Plan, as developed by the AMS Committee.

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

We intend to cover the OCS facilities in the Gulf of Mexico by a single, District-wide AMS Plan. The establishment of an AMS Committee for the OCS facilities in the Gulf of Mexico was discussed at recent Gulf Safety Committee and National Offshore Safety Advisory Committee (NOSAC) meetings. We intend to form an AMS Committee for this area in the near future. Additionally, owners and operators of OCS facilities are encouraged to participate on the AMS

Committee of the COTP zone that is most relevant to their operations.

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

The Maritime Transportation Security Act of 2002 (MTSA) requires full compliance with these regulations 1 year after the publication of the temporary interim rules, which were published on July 1, 2003. Therefore, a ''phased in approach'' will not be allowed. While compliance dates are mandatory, a vessel or facility owner or operator could ''gain relief'' from making physical improvements, such as installing equipment or fencing, by addressing the intended improvements in the Vessel or Facility Security Plan and explaining the equivalent security measures that will be put into place until improvements have been made.

We are amending the dates of compliance in § 106.110(a) and (b), § 106.115, and § 106.410(a) to align with the MTSA and the International Ship and Port Facility Security Code (ISPS Code) compliance dates.

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

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

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

One basis for the Coast Guard to establish security zones in the Exclusive Economic Zone (EEZ) is pursuant to the Ports and Waterways Safety Act, 33 U.S.C. 1221 *et seq.* For example, consistent with customary international law, 33 U.S.C. 1226 provides the Coast Guard with authority to carry out or require measures, including the establishment of safety and security zones, to prevent or respond to an act of terrorism against a vessel or public or commercial structure that is located within the marine environment. 33 U.S.C. 1222 defines ''marine environment'' broadly to include the waters and fishery resources of any area over which the United States asserts exclusive fishery management authority. The United States asserts exclusive fishery management authority in the EEZ.

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

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

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

*Subpart B—Outer Continental Shelf (OCS) Facility Security Requirements*

This subpart describes the responsibilities of the facility owner or operator and personnel relative to OCS facility security. It includes requirements for training, drills, recordkeeping, and Declarations of Security. It identifies specific security measures, such as those for access control, restricted areas, and monitoring.

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

We cannot establish only guidelines because the MTSA and the International Convention for Safety of Life at Sea, 1974 (SOLAS) require us to issue regulations. We have provided performance-based, rather than prescriptive, requirements in these regulations to give owners or operators flexibility in developing security plans tailored to vessels' or facilities' unique operations.

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

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

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

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

Administration (MARAD). MARAD has developed model training standards and curricula for maritime security personnel, including the Facility Security Officer. In addition, MARAD intends to develop course approval and certification requirements in the near future.

In the final rule for ''Vessel Security'' published elsewhere in today's **Federal Register** we made amendments to the responsibilities of the Company Security Officer. In this final rule, we are making conforming amendments to § 106.205(a)(2) to clarify that the Company Security Officer may also perform the duties of a Facility Security Officer.

Nine commenters requested formal alternatives to Facility Security Officers, Company Security Officers, and Vessel Security Officers much like the requirements of the Oil Pollution Act of 1990, that allow for alternate qualified individuals.

Parts 104, 105, and 106 provide flexibility for a Company, Vessel, or Facility Security Officer to assign security duties to other vessel or facility personnel under §§ 104.210(a)(4), 104.215(a)(5), 105.205(a)(3), and 106.210(a)(3). An owner or operator is also allowed to designate more than one Company, Vessel, or Facility Security Officer. Because Company, Vessel, or Facility Security Officer responsibilities are key to security implementation, vessel and facility owners and operators are encouraged to assign an alternate Company, Vessel, or Facility Security Officer to coordinate vessel or facility security in the absence of the primary Company, Vessel, or Facility Security Officer.

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

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

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

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

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

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

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

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

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

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

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

Two commenters requested that § 104.240(a) and (b)(1) be amended to specify that vessels must implement appropriate security measures before interfacing with facilities that are not located in a port. We agree that the vessel owner or operator, once notified of a change in MARSEC Level, must implement appropriate security measures before interfacing with a

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Two commenters asked us to amend § 106.250(f) to clarify that an expired Declaration of Security (§ 106.250(e)(2) or (e)(3)) must be replaced by a new Declaration of Security, in order for there to be a valid Declaration of Security.

Although we agree that an expired Declaration of Security must be replaced by a new Declaration of Security, in order for there to be a valid Declaration of Security, we believe that § 106.250 needs no further clarification. We do not preclude an OCS facility from executing a new Declaration of Security in accordance with § 106.250.

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

We recognize the seriousness of the commenters' concerns, but disagree that provisions for checking passenger and worker identification should be withdrawn. Identification checks, by themselves, may not ensure effective access control, but they can be critically important in attaining access control. Our rules implement the MTSA and the ISPS Code by requiring vessel and facility owners and operators to include access control measures in their security plans. However, instead of mandating uniform national measures, we leave owners and operators free to choose their own access control measures. In addition, our rules contain several provisions that work in favor of privacy. Identification systems must use disciplinary measures to discourage abuse. Owners and operators can take advantage of rules allowing for the use of alternatives, equivalents, and waivers. Passenger and ferry vessel owners or operators are specifically authorized to develop alternatives to passenger identification checks and screening. Signage requirements ensure that passengers and workers will have advance notice of their liability for screening or inspection. Vessel owners and operators are required to give particular consideration to the convenience, comfort, and personal privacy of vessel personnel. Taken as a whole, these rules strike the proper balance between implementing the MTSA's provisions for deterring transportation security incidents and preserving constitutional rights to privacy, travel, and association.

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

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

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

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

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

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

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

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

might not use the designated shoreside screening process.

We are amending § 104.265(b) to include a verb in the sentence for clarity. We are also mirroring this clarification in §§ 105.255(b) and 106.260(b).

We are amending § 106.265(c) to clarify the requirement by removing an extraneous word.

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

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

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

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

One commenter stated that the provision to mandate restricted areas on board OCS facilities should be removed from the rule, arguing that limiting access during an emergency should not be tolerated.

If the security assessment and plan for the OCS facility does not take into account access to restricted areas during an emergency situation, it may hinder effective response. Therefore, we have included several provisions to ensure that the security assessment and plan for the OCS facility address this issue, such as in §§ 106.205(d)(10), 106.280(b), and 106.305(c)(1)(vii).

One commenter suggested that this regulation contain provisions to allow vessels to continue fishing in or around OCS facilities. The commenter was concerned that any effort to prevent access to areas around these facilities would cause severe economic hardship to a large number of charterboat businesses.

The security regulations do not contain any provisions that specifically restrict fishing around OCS facilities. The OCS facility owner or operator may, however, restrict some areas as part of the facility's security measures. We do not believe that part 106 will cause a hardship for vessels that fish around OCS facilities because part 106 regulates only approximately 1 percent of all those facilities and because such restricted areas will likely be designated only during periods of heightened security.

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

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

*Subpart C—Outer Continental Shelf (OCS) Facility Security Assessment (FSA)*

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

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

Sections 104.405, 105.405, and 106.405 require that the security assessment report be submitted with the respective security plans. We believe that the security assessment report must be submitted as part of the security plan approval process because it is used to determine if the security plan adequately addresses the security requirements of the regulations. The information provided in form CG–6025 will be used to assist in the

development of AMS Plans. The security assessments are not required to be submitted. To clarify that the report, not the assessment, is what must be submitted with the Vessel or Facility Security Plan, we are amending § 104.305 to add the word ''report'' where appropriate. We have also amended §§ 105.305 and 106.305 for facilities and OCS facilities, respectively. Additionally we have amended these sections so that the Facility Security Assessment report requirements mirror the Vessel Security Assessment report requirements. All of these requirements were included in our original submission to OMB for ''Collection of Information'' approval, and there is no associated increase in burden in our collection of information summary. We also acknowledge that security assessments and security assessment reports have sensitive security information within them, and that they should be protected under §§ 104.400(c), 105.400(c), and 106.400(c). We are also amending §§ 104.305, 105.305, and 106.305 to clarify that all security assessments, security assessment reports, and security plans need to be protected from unauthorized disclosure. The Coast Guard has already instituted measures to protect sensitive security information, such as security assessment reports and security plans, from disclosure.

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

Portions of security plans are sensitive security information and must be protected in accordance with 49 CFR part 1520. Only those persons specified in 49 CFR part 1520 will be given access to sensitive security information portions of the security plans. In accordance with 49 CFR part 1520 and pursuant to 5 U.S.C. 552(b)(3), sensitive security information is exempt from disclosure under FOIA. However, §§ 104.220, 104.225, 105.210, 105.215, 106.215, and 106.220 of these rules state that vessel and facility personnel must have knowledge of relevant provisions of the security plan. Therefore, vessel and facility owners or operators will determine which provisions of the security plans are accessible to crewmembers and other personnel. Additionally, COTPs will determine what portions of the AMS Plan are accessible to Company or Facility Security Officers.

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

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

''Sensitive security information'' is a designation mandated by regulations promulgated by TSA and may be found in 49 CFR part 1520. These regulations state that information designated as sensitive security information may not be shared with the general public. FOIA exempts from its mandatory release provisions those items that other laws forbid from public release. Thus, security assessments, security assessment reports, and security plans, which should be designated as sensitive security information, are all exempt from release under FOIA.

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

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

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

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

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

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

collect information'' required to compile background information and ''consists of an actual survey that examines and evaluates existing vessel protective measures, procedures, and operations.'' An on-scene survey is part of a security assessment.

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

We agree with the commenter. The AMS Plan is more general in nature and takes into account those threats that may affect the entire port, or a segment of the port. As such, the AMS Plan should be designed to take into account those threats that are larger in scope than those threats that should be considered for individual facilities. To focus the Facility Security Assessments on their port interface rather than the broader requirement, we have amended §§ 105.305(c)(2)(viii), (ix) and 106.305 (c)(2)(v) to reflect that the assessment of the facility should take into consideration the use of the facility as a transfer point for a weapon of mass destruction and the impact of a vessel blocking the entrance to or area surrounding a facility.

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

We will not be providing a list of acceptable assessment companies, nor will we define ''appropriate skills.'' It is the responsibility of the vessel or facility owner or operator to vet companies that assist them in their security assessments. In the temporary interim rule (68 FR 39254) (part 101), we stated, ''we reference ISPS Code, part B, paragraph 4.5, as a list of competencies all owners and operators should use to guide their decision on hiring a company to assist with meeting the regulations. We may provide further guidance on competencies for maritime security organizations, as necessary, but do not intend to list organizations, provide standards within the regulations, or certify organizations.'' We require security assessments to be protected from unauthorized disclosures and will enforce this requirement, including through the penalties provision under § 101.415.

After further review of subpart C of parts 104, 105, and 106, we are amending §§ 104.310, 105.310, and 106.310 to state that the security assessment must be reviewed and updated each time the security plan is revised and when the security plan is submitted for reapproval.

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

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

*Subpart D—Outer Continental Shelf (OCS) Facility Security Plan (FSP)*

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

One commenter recommended that the interval for audits of the OCS Facility Security Plan be changed to biennial to be consistent with the audit requirements for emergency response plans.

The annual audit certifies that the OCS Facility Security Plan continues to meet the applicable requirements of part 106. We believe that annual audits are necessary because the OCS Facility Security Plan, as a living document, should be continuously updated to incorporate changes or lessons learned from drills and exercises.

Three commenters recommended that this rule be amended to close ''the gap'' in the plan-approval process to address the period of time between December 29, 2003, and July 1, 2004. Another commenter suggested submitting the Facility Security Plan for review and approval for a new facility ''within six months of the facility owner or operator's intent of operating it.''

We agree that the regulations do not specify plan-submission lead time for vessels, facilities, and OCS facilities that come into operation after December 29, 2003, and before July 1, 2004. The owners or operators of such vessels, facilities, and OCS facilities are responsible for ensuring they have the necessary security plans submitted and approved by July 1, 2004, if they intend to operate. We have amended §§ 104.410, 105.410, and 106.410 to clarify the plan-submission requirements for the various dates before July 1, 2004, and after this date.

Thirty commenters commended the Coast Guard for providing an option for an Alternative Security Program as described in § 101.120(b) and urged the Coast Guard to approve these programs as soon as possible.

We believe the provisions in § 101.120(b) will provide greater flexibility and will help owners and operators meet the requirements of these rules. We will review Alternative Security Program submissions in a timely manner to determine if they comply with the security regulations for their particular segment. Additionally, we have amended §§ 104.410(a)(2), 105.115(a), 105.410(a)(2), 106.110(a), and 106.410(a)(2), to clarify the submission requirements for the Alternative Security Program.

After further review of the ''Submission and approval'' requirements in §§ 101.120, 104.410, 105.410, and 106.410, we have amended the requirements to clarify that security plan submissions can be returned for revision during the approval process.

We received 15 comments about the process of amending and updating the security plans. Five commenters requested that they be exempted from auditing whenever they make minimal changes to the security plans. Two commenters stated that it should not be necessary to conduct both an amendment review and a full audit of security plans upon a change in ownership or operational control. Three commenters requested a *de minimis* exemption to the requirement that security plans be audited whenever there are modifications to the vessel or facility. Seven commenters stated that the rule should be revised to allow the immediate implementation of security measures without having to propose an amendment to the security plans at least 30 days before the change is to become effective. The commenters stated that there is something ''conceptually wrong'' with an owner or operator having to submit proposed amendments to security plans for approval when the amendments are deemed necessary to protect vessels or facilities.

The regulations require that upon a change in ownership of a vessel or facility, the security plan must be audited and include the name and contact information of the new owner or operator. This will enable the Coast Guard to have the most current contact information. Auditing the security plan is required to ensure that any changes in personnel or operations made by the new owner or operator do not conflict with the approved security plan. The

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

*Additional Changes*

During our review of this part, we noted that a section required a non-substantive editorial change, such as accurately completing a list. The section is § 106.275(a)(1). In addition, the part heading in this part has been amended to align with all the part headings within this subchapter.

**Regulatory Assessment**

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

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

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

*Cost Assessment*

For the purposes of good business practice or pursuant to regulations promulgated by other Federal and State agencies, many companies already have spent a substantial amount of money and resources to upgrade and improve security. The costs shown in this assessment do not include security measures these companies have already taken to enhance security. Because the changes in this final rule do not affect the original cost estimates presented in the temporary interim rule (68 FR 39341) (part 106), the costs remain unchanged.

The Coast Guard realizes that every company engaged in maritime commerce will not implement this final rule exactly as presented in the assessment. Depending on each company's choices, some companies could spend much less than what is estimated herein while others could spend significantly more. In general, the Coast Guard assumes that each company will implement this final rule differently based on the types of OCS facilities it owns or operates and whether it engages in international or domestic trade.

This final rule will affect about 40 OCS facilities under U.S. jurisdiction, (current and future OCS facilities). These OCS facilities engage in exploring for, developing, or producing oil, natural gas, or mineral resources. To determine the number of OCS facilities, we used data that the Mineral Management Service (MMS) has identified as nationally critical OCS oil and gas infrastructure. These OCS facilities meet or exceed any of the following operational threshold characteristics:

(1) OCS facility hosts more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more;

(2) Production greater than 100,000 (one hundred thousand) barrels of oil per day; or

(3) Production greater than 200,000,000 (two hundred million) cubic feet of natural gas per day.

The estimated cost of complying with the final rule is present value $37 million (2003–2012, 7 percent discount rate). In the first year of compliance, the cost of security assessments and plans, training, personnel, and paperwork is an estimated $3 million (non-discounted). Following initial implementation, the annual cost of compliance is an estimated $5 million (non-discounted).

Approximately 80 percent of the initial cost of the final rule is for assigning and establishing Company Security Officers and Facility Security Officers, 12 percent is associated with paperwork creating Facility Security Assessments and Facility Security Plans, and 8 percent of the cost is associated with initial training (not including quarterly drills). Following the first year, approximately 58 percent of the cost is training (including quarterly drills), 42 percent is for Company Security Officers and Facility Security Officers, and less than 1 percent is associated with paperwork. Annual training (including quarterly drills) is the primary cost driver of OCS facility security.

We estimated approximately 3,200 burden hours for paperwork during the first year of compliance (40 hours for each Facility Security Assessment and each Facility Security Plan). We estimated approximately 160 burden hours annually following full implementation of the final rule to update Facility Security Assessments and Facility Security Plans.

We estimated the cost of this final rule to be minimal in comparison to vessel and non-OCS facility security implementation. This final rule includes only personnel, training, and paperwork costs for the affected OCS facility population. We assume the industry is adequately prepared with equipment suited to be used for security purposes (lights, radios, communications), therefore no security equipment installation, upgrades, or maintenance will be required for this final rule.

*Benefit Assessment*

This final rule is one of six final rules that implement national maritime security initiatives concerning General Provisions, Area Maritime Security, Vessels, Facilities, OCS Facilities, and AIS. The Coast Guard used the National Risk Assessment Tool (N–RAT) to assess benefits that would result from increased security for vessels, facilities, OCS facilities, and areas. The N–RAT considers threat, vulnerability, and consequences for several maritime

entities in various security-related scenarios. For a more detailed discussion on the N–RAT and how we employed this tool, refer to ''Applicability of National Maritime Security Initiatives'' in the temporary interim rule titled ''Implementation of National Maritime Security Initiatives'' (68 FR 39243) (part 101). For this benefit assessment, the Coast Guard used a team to calculate a risk score for each entity and scenario before and after the implementation of required security measures. The difference in before and after scores indicated the benefit of the proposed action.

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

The Coast Guard determined annual risk points reduced for each of the final rules using the N–RAT. The benefits are apportioned among the Vessel, Facility, OCS Facility, AMS, and AIS requirements. As shown in Table 1, the implementation of OCS facility security for the affected population reduces 13,288 risk points annually through 2012. The benefits attributable for part 101, General Provisions, were not considered separately because it is an overarching section for all the parts.

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

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

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

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

| Item | Final rule | | | | |
|---|---|---|---|---|---|
| | Vessel security | Facility security | OCS facility security | AMS | AIS* |
| First-year cost (millions) | $218 | $1,125 | $3 | $120 | $30 |
| First-year benefit | 781,285 | 473,659 | 13,288 | 135,202 | 1,422 |
| First-year cost effectiveness ($/risk point reduced) | 279 | 2,375 | 205 | 890 | 21,224 |
| 10-Year present value cost (millions) | 1,368 | 5,399 | 37 | 477 | 26 |
| 10-Year present value benefit | 5,871,540 | 3,559,655 | 99,863 | 1,016,074 | 10,687 |
| 10-Year present value cost effectiveness ($/risk point reduced) | 233 | 1,517 | 368 | 469 | 2,427 |

*Cost less monetized safety benefit.

**Small Entities**

Under the Regulatory Flexibility Act (5 U.S.C. 601–612), the Coast Guard has considered whether this final rule would have a significant economic impact on a substantial number of small entities. The term ''small entities'' comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. The Coast Guard has reviewed this final rule for potential economic impacts on small entities. A Final Regulatory Flexibility Analysis discussing the impact of this final rule on small entities is available in the docket where indicated under **ADDRESSES.**

There are approximately 40 total current and future OCS facilities owned by five large companies that will be affected by this final rule. Depending on how the corporate headquarters' operation is classified and whether it is oil or gas specific, these companies are generally classified under the North American Industry Classification System (NAICS) code 211111 or 221210. According to the Small Business Administration guidelines for these industries, a company with less than 500 total corporate employees is considered a small entity. The entities affected by this final rule do not qualify as small entities because all of them have more than 500 employees.

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

**Assistance for Small Entities**

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121),

we offered to assist small entities in understanding the rule so that they could better evaluate its effects on them and participate in the rulemaking. We provided small entities with a name, phone number, and e-mail address to contact if they had questions concerning the provisions of the final rules or options for compliance.

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

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

**Collection of Information**

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

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

**Federalism**

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

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

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

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

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

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

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

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

**Unfunded Mandates Reform Act**

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

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

**Taking of Private Property**

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

**Civil Justice Reform**

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

**Protection of Children**

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

**Indian Tribal Governments**

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

**Energy Effects**

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

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

We did not receive comments regarding energy effects.

**Environment**

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

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

**List of Subjects in 33 CFR Part 106**

Facilities, Maritime security, Outer Continental Shelf, Reporting and recordkeeping requirements, Security measures.

■ Accordingly, the interim rule adding 33 CFR part 106, that was published at 68 FR 39338 on July 1, 2003, and amended at 68 FR 41916 on July 16, 2003, is adopted as a final rule with the following changes:

## PART 106—MARITIME SECURITY: OUTER CONTINENTAL SHELF (OCS) FACILITIES

■ 1. The authority citation for part 106 continues to read as follows:

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

■ 2. Revise the heading to part 106 to read as shown above.

■ 3. In § 106.110—

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

■ b. In paragraph (b), remove the date ''June 25, 2004'' and add, in its place, the date ''July 1, 2004'':

**§ 106.110 Compliance dates.**

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

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

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

Alternative Security Program the owner or operator intends to use.

* * * * *

**§ 106.115 [Amended]**

■ 4. In § 106.115—

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

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

■ 5. Revise § 106.120 to read as follows:

**§ 106.120 Noncompliance.**

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

■ 6. In § 106.200—

■ a. In paragraph (b)(7), remove the word ''and'';

■ b. In paragraph (b)(8), remove the period and add, in its place, the words ''; and''; and

■ c. Add paragraph (b)(9) to read as follows:

**§ 106.200 Owner or operator.**

* * * * *

(b) * * *

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

**§ 106.205 [Amended]**

■ 7. In § 106.205(a)(2), after the word ''organization'', add the words '', including the duties of a Facility Security Officer''.

**§ 106.220 [Amended]**

■ 8. In § 106.220, in the introductory paragraph, after the words ''of the following'', add the words '', as appropriate''.

■ 9. Revise § 106.225(a) to read as follows:

**§ 106.225 Drill and exercise requirements.**

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

(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the FSP as the result of an increase in the MARSEC Level, provided the FSO reports attainment to the cognizant District Commander.

* * * * *

**§ 106.230 [Amended]**

■ 10. In § 106.230(b)(1), remove the words ''each security training session'' and add, in their place, the words ''training under § 106.215''.

**§ 106.250 [Amended]**

■ 11. In § 106.250, in paragraph (d)—

■ a. After the words ''part 104'', add the words ''of this chapter, or their designated representatives,''; and

■ b. After the word ''DoSs'', add the words ''as required in paragraphs (b)(1) and (b)(2) of this section''.

**§ 106.260 [Amended]**

■ 12. In § 106.260—

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

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

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

**§ 106.265 [Amended]**

■ 13. In § 106.265(c), remove the words ''should include'' and add, in their place, the word ''includes''.

**§ 106.275 [Amended]**

■ 14. In § 106.275—

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

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

■ 15. In § 106.305—

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

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

**§ 106.305 Facility Security Assessment (FSA) requirements.**

* * * * *

(c) * * *

(2) * * *

(v) Effects of a nuclear, biological, radiological, explosive, or chemical attack to the OCS facility's shoreside support system;

* * * * *

(d) * * *

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

(i) OCS facility personnel;

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

(iii) OCS facility stores;

(iv) Any security communication and surveillance systems; and

(v) Any other security systems, if any.

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

(i) Conflicts between safety and security measures;

(ii) Conflicts between personnel duties and security assignments;

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

(iv) Security training deficiencies; and

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

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

(i) Ensuring performance of all security duties;

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

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

(iv) Supervising the delivery of stores and industrial supplies;

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

(vi) Monitoring deck areas and areas surrounding the OCS facility; and

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

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

■ 16. In § 106.310—

■ a. In paragraph (a), remove the words ''§ 106.405 of this part'' and add, in their place, the words ''§ 106.410 of this part''; and

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

**§ 106.310 Submission requirements.**

* * * * *

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

■ 17. In § 106.410, revise paragraph (a), introductory text, and paragraphs (a)(2), (b), and (c) to read as follows:

**§ 106.410 Submission and approval.**

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

* * * * *

(2) If intending to operate under an Approved Security Program, submit a

letter signed by the OCS facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

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

(c) The cognizant District Commander will examine each submission for compliance with this part and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

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

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

* * * * *

■ 18. In § 106.415, redesignate paragraph (a)(3) as paragraph (a)(4) and add new paragraph (a)(3) to read as follows:

**§ 106.415 Amendment and audit.**

(a) * * *

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

* * * * *

Dated: October 8, 2003.

**Thomas H. Collins,**

*Admiral, Coast Guard, Commandant.*

[FR Doc. 03–26349 Filed 10–20–03; 8:45 am]

**BILLING CODE 4910–15–U**

## DEPARTMENT OF HOMELAND SECURITY

### Coast Guard

### 33 CFR Parts 26, 161, 164, and 165

**[USCG–2003–14757]**

**RIN 1625–AA67**

## Automatic Identification System; Vessel Carriage Requirement

**AGENCY:** Coast Guard, DHS.

**ACTION:** Final rule.

**SUMMARY:** This final rule adopts, with changes, the temporary interim rule that amends port and waterway regulations and implements the Automatic Identification System (AIS) carriage requirements of the Maritime Transportation Security Act of 2002 (MTSA) and the International Maritime Organization requirements adopted under International Convention for the Safety of Life at Sea, 1974, (SOLAS) as amended.

This rule is one in a series of final rules published in today's **Federal Register**. To best understand this rule, first read the final rule titled ''Implementation of National Maritime Security Initiatives'' (USCG–2003–14792), published elsewhere in today's **Federal Register**.

**DATES:** This final rule is effective November 21, 2003. On July 1, 2003, the Director of the Federal Register approved the incorporation by reference of certain publications listed in this final rule.

**ADDRESSES:** Comments and material received from the public, as well as documents mentioned in this preamble as being available in the docket, are part of docket USCG–2003–14757 and are available for inspection or copying at the Docket Management Facility, U.S. Department of Transportation, room PL–401, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet at *http://dms.dot.gov.*

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

**FOR FURTHER INFORMATION CONTACT:** If you have questions on this final rule, call Mr. Jorge Arroyo, U.S. Coast Guard Office of Vessel Traffic Management (G–MWV), by telephone 202–267–6277, toll-free telephone 1–800–842–8740 ext. 7–6277, or electronic mail *jarroyo@comdt.uscg.mil.* If you have questions on viewing the docket, call Andrea M. Jenkins, Program Manager, Docket Operations, Department of Transportation, at telephone 202–366–0271.

**SUPPLEMENTARY INFORMATION:**

**Regulatory Information**

On July 1, 2003, we published a temporary interim rule with request for comments and notice of public meeting titled ''Automatic Identification System; Vessel Carriage Requirement'' in the **Federal Register** (68 FR 39353). This temporary interim rule was one of a series of temporary interim rules on maritime security published in the July 1, 2003, issue of the **Federal Register**. On July 16, 2003, we published a document correcting typographical errors and omissions in that rule (68 FR 41913).

We received a total of 438 letters in response to the six temporary interim rules by July 31, 2003. The majority of these letters contained multiple comments, some of which applied to the docket to which the letter was submitted, and some which applied to a different docket. For example, we received several letters in the docket for the temporary interim rule titled ''Implementation of National Maritime Security Initiatives'' that contained comments in that temporary interim rule, plus comments on the ''Automated Identification System; Carriage Requirement'' temporary interim rule. We have addressed individual comments in the preamble to the appropriate final rule. Additionally, we had several commenters submit the same comment to all six dockets. We counted these duplicate submissions as only one letter, and we addressed each comment within that letter in the preamble for the appropriate final rule. Because of statutorily imposed time constraints for publishing these regulations, we were unable to consider, in this Final Rule, comments received after the period for receipt of comments closed on July 31, 2003. Copies of late-received comments on AIS will be placed into the docket for the separate AIS Notice and request for comments that was published on July 1, 2003 (USCG 2003–14878; 68 FR 39369).

A public meeting was held in Washington, DC, on July 23, 2003, and approximately 500 people attended. Comments from the public meeting are also included in the ''Discussion of Comments and Changes'' section of this preamble. A transcript of this meeting is available in the docket, where indicated under **ADDRESSES.**

In order to focus on the changes made to the regulatory text since the temporary interim rule was published, we have adopted the temporary interim rule and set out, in this final rule, only the changes made to the temporary interim rule. We will place a copy of the unofficial complete regulatory text in