

DEPARTMENT OF HOMELAND SECURITY

COAST GUARD

33 CFR Parts 104, 160, and 165

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

[USCG-2003-14749]

RIN 1625-AA46

Vessel Security

AGENCY: Coast Guard, DHS.

ACTION: Temporary interim rule with request for comments and notice of meeting.

SUMMARY: This interim rule provides security measures for certain vessels calling on U.S. ports. It requires the owners or operators of vessels to designate security officers for vessels, develop security plans based on security assessments, implement security measures specific to the vessel's operation, and comply with Maritime Security Levels. This interim rule is one of six interim rules in today's Federal Register that comprise a new subchapter on the requirements for maritime security mandated by the Maritime Transportation Security Act of 2002. These six interim rules implement national maritime security initiatives concerning general provisions, Area

Maritime Security (ports), vessels, facilities, Outer Continental Shelf facilities, and the Automatic Identification System. Where appropriate, they align these domestic maritime security requirements with those of the International Ship and Port Facility Security Code and recent amendments to the International Convention for the Safety of Life at Sea. To best understand these interim rules, first read the interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792).

DATES:

Effective date. This interim rule is effective from [Insert date of publication in the FEDERAL REGISTER.] until November 25, 2003, with the exception of amendatory instructions 2, 5, 6, 8, 9, 10, 12, 14, 15, 16, 18, and 19 which are effective [Insert date of publication in the FEDERAL REGISTER]. The Coast Guard intends to finalize these amendments by November 25, 2003. On [Insert date 30 days after date of publication in the FEDERAL REGISTER.], the Director of the Federal Register approved the incorporation by reference of certain publications listed in this rule.

Comments. Comments and related material must reach the Docket Management Facility on or before. Comments on

collection of information sent to the Office of Management and Budget (OMB) must reach OMB on or before [Insert date 30 days after date of publication in the FEDERAL REGISTER.]

Meeting. A public meeting will be held on July 23, 2003, from 9 a.m. to 5 p.m., in Washington, D.C.

ADDRESSES:

Comments. To ensure that your comments and related material are not entered more than once in the docket, please submit them by only one of the following means:

(1) Electronically to the Docket Management System website at <http://dms.dot.gov>.

(2) By mail to the Docket Management Facility (USCG-2003-14749), U.S. Department of Transportation, room PL-401, 400 Seventh Street, SW., Washington, DC 20590-0001.

(3) By fax to the Docket Management Facility at 202-493-2251.

(4) By delivery to room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

You must also mail comments on collection of information to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street

NW., Washington, DC 20503, ATTN: Desk Officer, U.S. Coast Guard.

Meeting. A public meeting will be held on July 23, 2003 in Washington, D.C. at the Grand Hyatt Washington, D.C., 1000 H Street, N.W., Washington, D.C. 20001.

Availability. Electronic forms of all comments received into any of our dockets can be searched by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor unit, etc.) and is open to the public without restriction. You may also review the Department of Transportation's complete Privacy Act Statement in the Federal Register published on April 11, 2000 (65 FR 19477-78), or you may visit <http://dms.dot.gov/>.

FOR FURTHER INFORMATION CONTACT: If you have questions on this rule, call Lieutenant Kevin Oditt (G-MP), U.S. Coast Guard by telephone 202-267-1103, toll-free telephone 1-800-842-8740 ext. 7-1103, or electronic mail msregs@comdt.uscg.mil.

If you have questions on viewing or submitting material to the docket, call Ms. Dorothy Beard, Chief, Dockets, Department of Transportation, and telephone 202-366-5149.

SUPPLEMENTARY INFORMATION:

Due to the short timeframe given to implement these National Maritime Transportation Security initiatives, as directed by the Maritime Transportation Security Act (MTSA), and to ensure all comments are in the public venue for these important rulemakings, we are not accepting comments containing protected information for these interim rules. We request you submit comments, as explained in the Request for Comments section below, and discuss your concerns or support in a manner that is not security sensitive. We also request that you not submit proprietary information as part of your comment.

The Docket Management Facility maintains the public docket for this rulemaking. Comments and material received from the public, as well as documents mentioned in this preamble as being available in the docket, will become part of this docket and will be available for inspection or copying at room PL-401 on the Plaza level of the Nassif Building, 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>.

Request for Comments

We encourage you to participate in this rulemaking by submitting comments and related material. Your comments

will be considered for the final rule we plan to issue before November 25, 2003, to replace this interim rule. If you choose to comment on this rule, please include your name and address, identify the specific docket number for this interim rule (USCG-2003-14749), indicate the specific heading of this document to which each comment applies, and give the reason for each comment. If you have comments on another rule, please submit those comments in a separate letter to the docket for that rulemaking. You may submit your comments and material by mail, hand delivery, fax, or electronic means to the Docket Management Facility at the address under ADDRESSES. Please submit your comments and material by only one means. If you submit them by mail or hand delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during the comment period. We may change this rule in view of them.

Public Meetings

We will hold a public meeting on July 23, 2003, in Washington, D.C. at the Grand Hyatt Hotel, at the address listed under ADDRESSES. The meeting will be from 9 a.m. to

5 p.m. to discuss all of the maritime security interim rules, and the Automatic Identification System (AIS) interim rule, found in today's Federal Register. In addition, you may submit a request for other public meetings to the Docket Management Facility at the address under ADDRESSES explaining why another one would be beneficial. If we determine that other meetings would aid this rulemaking, we will hold them at a time and place announced by a later notice in the Federal Register.

Regulatory Information

We did not publish a notice of proposed rulemaking for this rulemaking and are making this rule effective upon publication. Section 102(d)(1) of the Maritime Transportation Security Act of 2002 (MTSA, Public Law 107-295, 116 STAT. 2064) requires the publication of an interim rule as soon as practicable without regard to the provisions of chapter 5 of title 5, U.S. Code (Administrative Procedure Act). The Coast Guard finds that harmonization of U.S. regulations with maritime security measures adopted by the International Maritime Organization (IMO) in December 2002, and the need to institute measures for the protection of U.S. maritime security as soon as practicable, furnish good cause for this interim rule to take effect immediately under both the Administrative

Procedure Act and section 808 of the Congressional Review Act.

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 interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792) published elsewhere in today's Federal Register.

Discussion of Comments Addressing Vessel Issues in the Notice of Meeting

For a discussion of comments on vessels at the public meetings and in the docket, see the interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792) published elsewhere in today's Federal Register.

Discussion of Interim Rule

This interim rule regulates the owners or operators of certain classes of vessels, in order to provide greater security to these vessels and to other vessels or ports with which a vessel interfaces. The interim rule adds part 104, Vessel Security, to the new subchapter H, Maritime Security of Title 33 of the Code of Federal Regulation. A general description of the process used in developing

subchapter H and its component parts appears in the interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792).

The MTSA and the International Ship and Port Facility Security (ISPS) Code use different terms to define similar, if not identical, persons or things. These differing terms sometimes match up with the terms used in subchapter H, but sometimes they do not. For a table of the terms used in subchapter H and their related terms in the MTSA and the ISPS Code, see the Discussion of Interim Rule section in the preamble for the interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792), published elsewhere in today's Federal Register.

The purpose of this rulemaking is to require certain vessels to perform security assessments, develop security plans, and implement security measures and procedures in order to reduce the risk of and to mitigate the results of an act that threatens the security of the crew, the vessel, or the public. This rulemaking combines international requirements and existing domestic policy and is published as a part of a new subchapter on maritime security. The MTSA mandates vessels that are required to conduct security assessments and develop security plans to submit their vessel security plan within six months of the publication

of this interim rule. It also mandates that the vessels shall be in compliance with their approved security plan within 12 months of the publication of this interim rule. However, consistent with customary international law, the requirements in part 104 do not apply to vessels engaged in innocent passage through the territorial sea of the U.S. or in transit passage through the navigable waters of the U.S. that form part of an international strait.

Part 104 consists of four subparts: subpart A (General), subpart B (Vessel Security Requirements), subpart C (Vessel Security Assessment), and subpart D (Vessel Security Plan). Where appropriate, the requirements discussed in part 104 are consistent with requirements in the ISPS Code, and include the requirements discussed below.

Compliance.

U.S. flag vessel compliance with this part will be verified during inspections by the Coast Guard as provided in 46 CFR part 2. 46 CFR subchapters D, H, I, K, L, and T will be amended to require that a certificate of inspection be based on the condition that the vessel meets the requirements of 33 CFR subchapter H and specifically this part.

Foreign vessels that have on board a valid International Ship Security Certificate that attests to the vessel's compliance with International Convention for Safety of Life at Sea, 1974, (SOLAS) and the ISPS Code, part A, and the relevant provisions in the ISPS Code, part B, of will be deemed in compliance with this part, except for those sections otherwise specified. Foreign vessel compliance will be verified during Port State Control verification exams.

The interim rule also affects the Notice of Arrival rule in part 160 of title 33, U.S. Code. These changes provide the Coast Guard with additional information essential to our exercise of Port State Control functions and to our imposition of control and compliance measures on foreign vessels bound for a port or place in the U.S., consistent with MTSA and with SOLAS regulation XI-2/9. A foreign vessel already covered by the Notice of Arrival rule will have to provide information about its International Ship Security Certificate and its implementation of an approved security plan.

As required by SOLAS Chapter XI-2 Regulation 3 and the ISPS Code, part A, section 5, the Coast Guard has published additional requirements for vessels calling in the U.S. in §§ 104.240 and 104.255 of 33 CFR 104. These sections

provide the U.S. requirements for setting and communicating changes in Maritime Security Level, completing Declarations of Security, and additional instructions for all vessels when Maritime Security Level 3 is set.

Waivers.

The waiver section details procedures for requesting a waiver for the benefit of vessel owners or operators who find specific requirements of the rulemaking to be unnecessary.

Equivalents.

The equivalents section details procedures for requesting an equivalency for specific requirements of the rulemaking. Equivalents are intended to allow vessel owners or operators to provide an alternative provision or arrangement that provides the same level of security as a specific requirement contained within this part.

Alternative Security Program.

This part makes provision to allow owners or operators of vessels on domestic voyages only to implement an Alternative Security Program that has been reviewed and accepted by the Commandant (G-MP), to meet the requirements of this part. Alternative Security Programs must be comprehensive and based on a security assessment to demonstrate it meets the intent of each section of this

part. Owners or operators are required to implement an appropriate Alternative Security Program in its entirety to be deemed in compliance with this part.

We also strongly encourage industry groups to develop and submit "model programs," which would include a model Vessel Security Plan and assessment of their own. A model program is one that, once submitted and reviewed and approved by Commandant (G-MP), may be used as a template for other vessels in the fleet. However, a Vessel Security Plan constructed using a model plan would still require submission for approval by the Coast Guard.

The process of the review and acceptance of model programs will be the same as the process used for the Alternative Security Program. The submission of a model program will need to include a general assessment for the applicable segment of the industry for which the model program is intended. The submission must also include how owners or operators will implement the model program including performing an operational and vessel-specific assessment and verification of implementation. Once these model programs are accepted, the programs could be used by industry to develop vessel-specific plans and assessments for Coast Guard approval.

Evaluating Submissions of Waivers, Equivalents, and
Alternative Security Programs.

In our evaluation of waivers, equivalencies, and Alternative Security Programs, the Coast Guard will accept a self-assessment or demonstration using any risk management tools acceptable to the Coast Guard. This demonstration may be requested to show that the proposed waiver, equivalency or Alternative Security Program is at least as effective as that intended by this interim rule.

Owner or Operator Responsibilities.

The owner or operator of a vessel is generally responsible for all requirements imposed by this part. These requirements include ensuring the following: the performance of all vessel security duties; defining the security organizational structure for each vessel; providing each person(s) exercising security duties or responsibilities within that structure with the support needed to fulfill those obligations; that personnel receive training, drills, and exercises enabling them to perform their assigned security duties; and that adequate coordination of security issues between vessels and facilities take place.

Company Security Officer (CSO).

This interim rule requires that each vessel owner or operator appoint a Company Security Officer, designated in writing, for their fleet of vessels or for each individual vessel that is owned or operated by the company. The Company Security Officer may be a full time or collateral position. A Company Security Officer may perform other duties within the owner's or operator's organization provided he or she is able to perform the duties and responsibilities required of the Company Security Officer. The Company Security Officer may also be the Vessel Security Officer, provided he or she is also able to perform the duties and responsibilities required of the Company Security Officer. Generally, this provision is for vessels operating on restricted routes in a single COTP zone and for unmanned vessels.

The Company Security Officer must have a general knowledge in a range of issues, such as company security organization, relevant international laws, domestic regulations, current security threats and patterns, risk assessment methodology, and in conducting audits, inspections, and control procedures.

The CSO may delegate the duties imposed on the Company Security Officer by this part, but remains responsible for

the performance of those duties. The most important duties of the Company Security Officer include ensuring that: a Vessel Security Assessment is conducted; a Vessel Security Plan is developed, approved, maintained, and implemented; the Vessel Security Plan is modified when necessary; vessel security activities are audited as appropriate; problems identified by audits or inspections are addressed in a timely fashion; adequate security training; and communication and cooperation between the vessel and facilities.

Vessel Security Officer (VSO).

This interim rule requires that a Vessel Security Officer is designated in writing for each vessel. The Vessel Security Officer must have a general knowledge in a range of issues, such as security administration, relevant international laws, domestic regulations, current security threats and patterns, risk assessment methodology, and in conducting audits, inspections, and control procedures. The most important duties that must be performed by the Vessel Security Officer includes implementing a Vessel Security Plan; ensuring that adequate training is provided to vessel personnel; ensuring the vessel is operating in accordance with the plan and in continuous compliance with part 104; and periodically auditing and updating the Vessel

Security Assessment and Vessel Security Plan. The Vessel Security Officer may assign security duties to other vessel personnel; however, the Vessel Security Officer remains responsible for security duties.

Training.

Required training for vessel personnel must be specified in the Vessel Security Plan. Specific security training courses for the Vessel Security Officer and vessel personnel will not be required by the Coast Guard. While formal training may be necessary, we will not mandate specifics. Vessel owners or operators must certify that security personnel are, in fact, properly trained to perform their duties. The types of training required must also be consistent with the training requirements described in this subpart. The Vessel Security Officer is also required to ensure that vessel security persons possess necessary training to maintain the overall security of the facility.

Drills and Exercises Requirements.

Exercises are required to ensure the adequacy of the Facility Security Plans and are required to be conducted at least once each calendar year, with not more than 18 months between exercises. Drills, which are smaller in scope than exercises, must be conducted at least every three months.

Exercises may be vessel specific, or as part of a cooperative exercise program with applicable Facility and Vessel Security Plans or Port exercises. Exercises for security may be combined with other required exercises, as appropriate.

Security Systems and Equipment Maintenance.

Procedures and/or policies must be developed and implemented to ensure security systems and equipment are tested and operated in accordance with the instructions of the manufacturer and ready for use.

Security Measures.

Security measures for specific activities must be scalable in order to provide increasing levels of security at increasing Maritime Security (MARSEC) Levels. An effective security program relies on detailed procedures that clearly indicate the preparation and prevention activities that will occur at each threat level and the organizations, or personnel, who are responsible for carrying out those activities. Security Measures must be developed for the following activities:

- Security measures for access control;
- Security measures for restricted areas;
- Security measures for handling cargo;

- Security measures for delivery of vessel stores and bunkers; and
- Security measures for monitoring.

Security Incident Procedures.

Each vessel owner or operator must develop security incident procedures for responding to transportation security incidents. The security incident procedures must explain the vessel's reaction to an emergency, including the notification and coordination with local, State, and federal authorities and Under Secretary of Emergency Preparedness and Response. The security incident procedures must also explain actions for securing the vessel and evacuating passengers and crew.

Declaration of Security (DoS).

A Declaration of Security provides a means for ensuring that critical security concerns are properly addressed prior to and during a vessel-to-facility interface. The Declaration of Security addresses security by delineating responsibilities for security arrangements and procedures between a vessel and a facility. This requirement is similar to the existing U.S. practice for vessel-to-facility oil transfer proceedings.

Only certain passenger vessels and vessels carrying Certain Dangerous Cargoes will complete a Declaration of

Security for every evolution regardless of the Maritime Security Level. At Maritime Security Levels 2 and 3, all vessels and facilities would need to complete the Declaration of Security.

Vessels that frequently call on the same facility may execute a continuing Declaration of Security - a single Declaration of Security for multiple visits.

All Declarations of Security must state the security activities for which the facility and vessel are responsible during vessel-to-vessel or vessel-to-facility interfaces. Declarations of Security must be kept as part of the vessel's recordkeeping.

Vessels that are operating at a higher Security Level than the port that the vessel is calling at may request a Declaration of Security with the facility, and the facility must complete a Declaration of Security with the vessel. Additionally, a facility may request that a vessel complete a Declaration of Security with the facility as appropriate for that facility's Security Plan or direction of the COTP. If the facility owner or operator requires a Declaration of Security, the vessel must comply. The conditions under which a vessel may request a Declaration of Security from the facility must be included in the Vessel Security Plan.

Vessel Security Assessment (VSA).

This interim rule requires all vessels covered by part 104 to conduct a Vessel Security Assessment, which is an essential and integral part of the process for developing and updating the required Vessel Security Plan. The Vessel Security Assessment is based in part on an on-scene security survey, which details the overall assessment of the vessel including any existing security measures, and includes a written report documenting the vulnerabilities and mitigation strategies of the vessel. As discussed in the interim rule "Implementation of National Maritime Security Initiatives" (USCG-2003-14792), 33 CFR 101.510 lists the various assessment tools that may be used to meet the risk assessment requirements in parts 104 through 106 of this subchapter. The assessment tools listed are sufficient to enable the development of the Vessel Security Program. This list is also provided to ensure that the Vessel Security Assessment is consistent with other modal assessments. We are working with other agencies to develop assessment tools that are sensitive to the diversity of the National Marine Transportation System to ensure consistent levels of security throughout the entire System. The designated Company Security Officer must conduct the on-scene survey by examining and evaluating existing vessel

protective measures, procedures, and operations. Using the information obtained in the on-scene survey, the Company Security Officer must ensure the completion the Vessel Security Assessment. The Vessel Security Assessment identifies and evaluates, in writing, existing security measures; key vessel operations; the likelihood of possible threats to key vessel operations; and weaknesses, including human factors in the infrastructure, policies, and procedures of the vessel.

It also includes a written summary of how the assessment was conducted; each vulnerability found during the assessment; and countermeasures that could be used to address each vulnerability. The Vessel Security Assessment must be reviewed and updated each time the Vessel Security Plan is revised and when the Vessel Security Plan is submitted for re-approval every five years.

Vessel Security Plan (VSP).

This interim rule requires each vessel owner or operator to develop an effective Vessel Security Plan that incorporates detailed preparedness, prevention, and response activities for each Maritime Security Level, along with the organizations or personnel responsible for carrying out those activities. The requirements discussed

in this part are consistent with requirements in the ISPS Code.

The Vessel Security Plan is a document, written in English, that is prepared in response to the Vessel Security Assessment and approved by the Coast Guard. A single Vessel Security Plan can apply to more than one vessel to the extent that they share physical characteristics and operations.

In addition to other things, the Vessel Security Plan must: respond specifically to any recommendations made by the Vessel Security Assessment; describe how, at each Maritime Security Level, the vessel will apply the security measures required in these regulations; state the Master's authority; must detail the organizational structure of security for the vessel; detail the duties and responsibilities of all vessel and company personnel with a security role; detail the vessel's relationship with the Company, facilities, other vessels, and relevant authorities with security responsibility; provide regular audit of the Vessel Security Plan and its amendment in response to experience or changing circumstances; and establish the procedures needed to assess the continuing effectiveness of security procedures and all security related equipment and systems, including procedures for

identifying and responding to equipment or systems failure or malfunction.

The responsibility for barge security lies not only with the barge owner or operator but also with the towing vessel, fleeting facility, and facility where the barge is moored. Hence, security plans for vessels and facilities that interface with unmanned vessels (e.g. unmanned barges) must include additional provisions to address the risk of the unmanned vessels that they will receive or handle. Given the simple design of a typical barge and the wide range of products that may be transported within a single tow or moored within a single fleeting area, the security assessments of facilities and towing vessels should include the barge sizes and cargos that would result in a worst-case scenario (i.e. greatest potential consequence due to cargo volatility, toxicity, or environmental damage), and the most probable vulnerability scenarios.

Vessel and facility security plans must address how the vessel or facility will apply the necessary security measures when engaged with a barge. Therefore, the security plans need to include procedures and security measures to protect the towing vessel or the facility that controls the barge(s). In addition, the security plans need to include procedures for interfacing with other

vessels and facilities, including how it will transfer custody of the barge to the next facility or towing vessel.

Facilities and towing vessels are not required to have a copy of the security plan for each barge it handles if the facility or towing vessel security plan includes appropriate procedures and security measures to ensure the security of all barges in its care. It is the responsibility of all Security Officers (barge's Vessel Security Officer, the towing vessel's Vessel Security Officer, the Company Security Officer, and the Facility Security Officer) to coordinate plans and ensure, possibly through a written contract or other agreement, that each party that receives the barge understands and is capable of implementing specific security measures for it. This may entail providing a copy of the applicable sections of a barge's Vessel Security Plan to the parties involved.

As a result, a barge's Vessel Security Plan may be minimal in content, containing personnel contact information and an assessment of the worst-case damage it might produce. The security plan must explain how security will be coordinated with each towing vessel, fleeting facility, and facility that handles the barge. Existing plans and procedures, such as vessel response plans, may be used or referenced as part of the Vessel Security Plan.

Like other Vessel Security Plans, the barge's Vessel Security Plan must also include specific security incident procedures to mitigate the consequences of damage and/or a release of the barge's cargo.

Foreign vessels required to comply with SOLAS are not required to submit their Vessel Security Plans to the Coast Guard for approval. Pursuant to SOLAS and the ISPS Code, these plans are required to be approved by the flag administration or Recognized Security Organization (RSO). Approval can only be granted by the flag administration or the RSO after verification that the Vessel Security Plan meets the requirements of SOLAS and the ISPS Code, part A, taking into account the ISPS Code, part B. Even so, the Coast Guard will verify that foreign SOLAS vessels have an approved Vessel Security Plan that fully complies with SOLAS and the ISPS Code, and thereby meets the requirements of this part, through an aggressive Port State Control program. Noncompliance will subject the vessel to a range of control and compliance measures, which could include denial of entry into port. If, during an expanded examination, those sections of the Vessel Security Plan the port state is allowed to review are not written in English, a vessel may be delayed while translator services are acquired. To properly reflect the full range of legal

authorities to control vessel movement in such cases, and without affecting other legal authorities, this rule amends the authority provision in 33 CFR part 165 to cite the anti-terrorism authorities in 33 U.S.C. 1226 as an additional basis for taking action under 33 CFR part 165.

However, in certain cases foreign vessel owners or operators will be required to submit the Vessel Security Plan to the U.S. for approval. Generally, these vessels fall into three categories: (1) a commercial vessel meeting the applicability standards of these regulations from a nation not signatory to SOLAS; (2) Canadian commercial vessels operating solely on the Great Lakes that (a) are greater than 100 gross register tons or (b) carry more than 12 passengers; and (3) other foreign commercial vessels meeting the applicability standards of this part, but below 500 gross tonnage, ITC and above 100 gross register tons.

Submission and Approval of Security Plan.

The Vessel Security Plan, including the Vessel Security Assessment report, must be submitted to and reviewed by the Commanding Officer, Marine Safety Center (MSC). Once the MSC finds that the plan meets the security requirements in part 104, the submitter will receive an approval letter that may contain conditions of the approval.

If the MSC requires more time than is indicated in the requirements of the interim rule to review a submitted Vessel Security Plan, the MSC may return to the submitter a written acknowledgement stating that the Coast Guard is currently reviewing the Vessel Security Plan submitted for approval, and that the vessel may continue to operate so long as the vessel remains in compliance with the submitted Vessel Security Plan.

If the MSC finds that the Vessel Security Plan does not meet the security requirements, the plans would be returned to the vessel with a disapproval letter with an explanation of why the plan does not meet the part 104 requirements.

The Coast Guard must review Vessel Security Plans every time:

- The Vessel Security Assessment is altered;
- Failures are identified during an exercise of the Vessel Security Plan; and
- There is a change in ownership or operational control of the vessel or there are amendments to the Vessel Security Plan.

Existing Regulations.

33 CFR part 120, Security of Vessels, currently exists but applies only to cruise ships. Until July 2004, 33 CFR

part 120 will remain in effect. Vessels that were required to comply with part 120 will now also be required to meet the requirements of this part including § 104.295, titled Additional requirements--Cruise Ships. The requirements in § 104.295 generally capture the existing requirements in part 120 that are specific for cruise ships and captures additional detail to the requirements of SOLAS Chapter XI-2 and the ISPS Code.

The Coast Guard Notice of Arrival regulation, 33 CFR part 160, is being amended by this interim rule to require the advance submission of additional security related information. This information is essential to assist Coast Guard officials in exercising Port State Control functions, including what control and compliance measures, if any, should be imposed on vessels bound for a port or place in the U.S., consistent with 46 U.S.C. 70103 and 70110 or SOLAS regulation XI-2/9.

The Notice of Arrival amendments also provide an initial indication to the U.S. that owners and operators are taking responsibility for fully complying with the requirements in this part. For example, vessels will be required to provide a statement that the vessel is in compliance with the ISPS Code prior to entry into ports in the U.S. by informing the National Vessel Movement Center

of the type and status of its International Ship Security Certificate. Those vessels required to have on board an approved Vessel Security Plan will also have to declare in the Notice of Arrival submission that they are implementing their Vessel Security Plan. Furthermore, because it is not the intent of the ISPS Code to allow consecutive Interim International Ship Security Certificates, the owner or operator of a vessel holding a consecutive Interim International Ship Security Certificate will also be required to provide an explanation as to why the vessel holds a consecutive Interim International Ship Security Certificate prior to entry.

The information we are requiring in this Notice of Arrival amendment contains elements similar to those we mandate to verify compliance with the International Management Code for the Safe Operation of Ships and for Pollution Prevention. Most of this information will be required only after the new SOLAS amendments and ISPS Code go into effect, in July 2004. However, after January 1, 2004, if a foreign vessel already possesses an International Ship Security Certificate and an approved Vessel Security Plan, we will require it to provide some basic information about the International Ship Security Certificate and declare if it is implementing the Vessel

Security Plan. The purpose of collecting this data in the first half of 2004 is to help us gauge international progress toward meeting the July 1, 2004, entry into force date.

Regulatory Assessment

This interim rule is a "significant regulatory action" under section 3(f) of Executive Order 12866, Regulatory Planning and Review, and has been reviewed by the Office of Management and Budget 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 Cost Assessment is available in the docket as indicated under ADDRESSES.

Cost Assessment

For the purposes of good business practice or regulations promulgated by other Federal and State agencies, many companies already have spent a substantial amount of money and resources to upgrade and improve security. The costs shown in this assessment do not include the security measures these companies have already taken to enhance security.

We realize that every company engaged in maritime commerce would not implement the interim rule exactly as

presented in this assessment. Depending on each company's choices, some companies could spend much less than what is estimated herein while others could spend significantly more. In general, we assume that each company would implement the interim rule based on the type of vessels or facilities it owns or operates and whether it engages in international or domestic trade.

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

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

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

The estimated cost of complying with the interim rule is Present Value (PV) \$1.368 billion (2003-2012, 7 percent discount rate). Approximately PV \$248 million of this total is attributable to U.S. flag SOLAS vessels. Approximately PV \$1.110 billion is attributable to domestic

vessels (non-SOLAS), and PV \$10 million is attributable to foreign non-SOLAS vessels. In the first year of compliance, the cost of purchasing equipment, hiring security officers, and preparing paperwork is an estimated \$218 million (non-discounted, \$42 million for the U.S. flag SOLAS fleet, \$175 million for the domestic fleet, \$1 million for the foreign non-SOLAS fleet). Following initial implementation, the annual cost of compliance is an estimated \$176 million (non-discounted, \$32 million for the U.S. flag SOLAS fleet, \$143 million for the domestic fleet, \$1 million for the foreign non-SOLAS fleet).

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

For the domestic fleet, approximately 51 percent of the initial cost is for hiring Company Security Officers and training personnel, 29 percent is for vessel equipment, 14 percent is for assigning Vessel Security Officers to vessels, and 6 percent is associated with paperwork (Vessel Security Assessments and Vessel Security Plans). Following the first year, approximately 61 percent of the cost is for Company Security Officers and training, 6 percent is for vessel equipment, 11 percent is for drilling, 22 percent is for VSOs, and less than 1 percent is associated with paperwork. As with SOLAS vessels, Company Security Officers are the primary cost driver for the domestic fleet.

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

We also estimated the annual cost for going to an elevated security level, Maritime Security Level 2, in response to increased threats. The duration of the increased security level will be entirely dependent on

intelligence received. For this assessment, we estimated costs for Maritime Security Level 2 using the following assumptions: all ports will go to Maritime Security Level 2 at once, each elevation will last 21 days, and the elevation will occur twice a year. The estimated cost associated with these conditions is \$235 million annually.

Benefit Assessment

This interim rule is one of six interim rules that implement national maritime security initiatives concerning general provisions, Area Maritime Security (ports), vessels, facilities, Outer Continental Shelf (OCS) facilities, and AIS. The Coast Guard used the National Risk Assessment Tool (N-RAT) to assess benefits that would result from increased security for vessels, facilities, OCS facilities, and ports. 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 interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792), published elsewhere in today's Federal Register. 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 interim 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 rulemaking 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 interim rule titled “Implementation of National Maritime Security Initiatives” (USCG-2003-14792) published elsewhere in today’s Federal Register.

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

Table 1. Annual Risk Points Reduced by the Interim Rules.

Maritime Entity	Annual Risk Points Reduced by Rulemaking				
	Vessel Security Plans	Facility Security Plans	OCS Facility Security Plans	AMS Plans	AIS
Vessels	778,633	3,385	3,385	3,385	1,448
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	1,553

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 PV cost and the 10-year PV benefit. The results of our assessment are presented in Table 2.

Table 2. First-Year and 10-Year PV Cost and Benefit of the Interim Rules.

Item	Interim Rule				
	Vessel Security Plans	Facility Security Plans	OCS Facility Security Plans	AMS Plans	AIS*
First-Year Cost (millions)	\$218	\$1,125	\$3	\$120	\$41
First-Year Benefit	781,285	473,659	13,288	135,202	1,553
First-Year Cost Effectiveness (\$/Risk Point Reduced)	\$279	\$2,375	\$205	\$890	\$26,391
10-Year PV Cost (millions)	\$1,368	\$5,399	\$37	\$477	\$42
10-Year PV Benefit	5,871,540	3,559,655	99,863	1,016,074	11,671
10-Year PV Cost Effectiveness (\$/Risk Point Reduced)	\$233	\$1,517	\$368	\$469	\$3,624

*Cost less monetized safety benefit.

Small Entities

Under the Regulatory Flexibility Act (5 U.S.C. 601-612), we considered whether this interim 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. This interim rule does not require a general notice of proposed rulemaking and, therefore, is exempt from the requirements of the Regulatory Flexibility Act. Although this interim rule is exempt, we have reviewed it for potential economic impacts

on small entities. An Initial Regulatory Flexibility Analysis discussing the impact of this interim rule on small entities is available in the docket where indicated under ADDRESSES.

U.S. Flag SOLAS Vessels.

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

Table 3. Estimated revenue impacts for small businesses that own U.S. flag SOLAS vessels.

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

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

Domestic Vessels.

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

revenue impacts following the first year, when companies will have the assessments and plans complete, but will need to conduct quarterly drilling.

Table 4. Estimated revenue impacts for small businesses that own domestic vessels.

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

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

Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Public Law 104-121), we want to assist small entities in understanding this interim rule so that they can better evaluate its effects on them and participate in the rulemaking. If the interim rule would affect your small business, organization, or

governmental jurisdiction and you have questions concerning its provisions or options for compliance, please consult Lieutenant Kevin Oditt (G-MP), U.S. Coast Guard by telephone 202-267-1103, toll-free telephone 1-800-842-8740 ext. 7-1103, or electronic mail msregs@comdt.uscg.mil.

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 interim rule calls for a collection of information 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 title and description of the information collections, a description of those who must collect the information, and an estimate of the total annual burden follow. The estimate covers the time for

reviewing instructions, searching existing sources of data, gathering and maintaining the data needed, and completing and reviewing the collection.

This interim rule modifies two existing OMB-approved collections--1625-0077 [formerly 2115-0622] and 1625-0100 [formerly 2115-0557]. Summaries of the revised collections follow.

TITLE: Security Plans for Ports, Vessels, Facilities, and Outer Continental Shelf Facilities and Other Security-Related Requirements.

OMB CONTROL NUMBER: 1625-0077

SUMMARY OF THE COLLECTION OF INFORMATION: The Coast Guard requires security assessments and plans for vessels. This interim rule provides a framework to ensure adequate security planning, drilling, and communication procedures by requiring vessels to develop and submit for approval Vessel Security Assessments and Vessel Security Plans.

NEED FOR INFORMATION: The primary need for information is to identify the adequate security mitigating measures that will be implemented when needed.

PROPOSED USE OF INFORMATION: The information will be used to identify and communicate the security mitigating measures to the Coast Guard and necessary personnel.

DESCRIPTION OF THE RESPONDENTS: The Company Security Officer for owners and operators of the affected vessels or

another designated person is responsible for developing the Vessel Security Assessment and the Vessel Security Plan.

NUMBER OF RESPONDENTS: 2,202 Company Security Officers at the affected companies.

FREQUENCY OF RESPONSE: Vessel Security Assessments and Vessel Security Plans are to be submitted for approval initially, and will be reviewed annually.

BURDEN OF RESPONSE: Development burden for the Vessel Security Assessments and Vessel Security Plans is estimated to be approximately eight to 80 hours depending on the size of the company and the number and types of vessels the company owns. Updating the assessments and plans is estimated to be approximately one to four hours depending on the size of the company and the number and types of vessels the company owns.

ESTIMATE OF TOTAL ANNUAL BURDEN: Vessel Security Assessments and Vessel Security Plans will have a total burden in the initial year of 135,269 hours. Annually, the total burden of the assessments and the plans is 11,700 hours. For a summary of all revisions to this existing OMB-approved collection, refer to Collection of Information in the interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792) published elsewhere in today's Federal Register.

TITLE: Advance Notice of Arrival.

OMB CONTROL NUMBER: 1625-0100

SUMMARY OF THE COLLECTION OF INFORMATION: The Coast Guard requires pre-arrival messages from any vessel entering a port or place in the United States. This interim rule adds the requirement to communicate security-related information about the vessel to the Coast Guard.

NEED FOR INFORMATION: The primary need for information is to identify the adequate security mitigating measures that will be implemented when needed.

PROPOSED USE OF INFORMATION: The information will be used to identify and communicate the security mitigating measures to the Coast Guard and necessary personnel.

DESCRIPTION OF THE RESPONDENTS: Respondents are owners and operators of vessels that arrive at or depart from a port or place in the United States after departing from foreign ports.

NUMBER OF RESPONDENTS: The existing OMB-approved collection number of respondents is 10,367. This rule will not increase the number of respondents.

FREQUENCY OF RESPONSE: The existing OMB-approved collection number of responses is 68,289. This rule will not increase the number of responses.

BURDEN OF RESPONSE: The existing OMB-approved collection burden of response is approximately 2.5 hours. Because the already approved Cargo Declaration requirement (Table 160.206(a)(8), per Final Rule of May 22, 2003; USCG-2002-11865; 68 FR 27908) has been suspended, this rule will not have a net increase in the burden.

ESTIMATE OF TOTAL ANNUAL BURDEN: The existing OMB-approved total annual burden is 174,179 hours. This rule will not increase the burden. However, due to an adjustment in the way the Coast Guard calculates the burden, we estimate the total annual burden to be 173,904.

As required by the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)), we have submitted a copy of this interim rule to the Office of Management and Budget (OMB) for its review of the collection of information. Due to the circumstances surrounding this temporary rule, we asked for "emergency processing" of our request. We received OMB approval for these collections of information on June 16, 2003. They are valid until December 31, 2003.

We ask for public comment on the collection of information to help us determine how useful the information is; whether it can help us perform our functions better; whether it is readily available elsewhere; how accurate our estimate of the burden of collection is; how valid our

methods for determining burden are; how we can improve the quality, usefulness, and clarity of the information; and how we can minimize the burden of collection.

If you submit comments on the collection of information, submit them both to OMB and to the Docket Management Facility where indicated under ADDRESSES, by the date under DATES.

You need not respond to a collection of information unless it displays a currently valid control number from OMB. We received OMB approval for these collections of information on June 16, 2003. They are valid until December 31, 2003.

Federalism

An interim rule has implications for federalism under Executive Order 13132, Federalism, if it has a substantial direct effect on State or local governments and would either preempt State law or impose a substantial direct cost of compliance on them. See the Federalism section in the interim rule preamble titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792) published elsewhere in today's Federal Register for a discussion of our analysis under this Executive Order.

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 tribal government, in the aggregate, or by the private sector of \$100,000,000 or more in any one year. This interim rule is exempted from assessing the effects of the regulatory action as required by the Act because it is necessary for the national security of the U.S. (2 U.S.C. 1503(5)).

Taking of Private Property

This interim 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.

Civil Justice Reform

This interim 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.

Protection of Children

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

Indian Tribal Governments

This interim 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.

Energy Effects

We have analyzed this interim 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 interim rule has a positive effect on the supply, distribution, and use of energy. The interim 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.

Trade Impact Assessment

The Trade Agreement Act of 1979 (19 U.S.C. 2501-2582) prohibits Federal agencies from engaging in any standards or related activities that create unnecessary obstacles to the foreign commerce of the U.S. Legitimate domestic objectives, such as safety and security, are not considered unnecessary obstacles. The Act also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. We have assessed the potential effect of this interim rule and have determined that it would likely create obstacles to the foreign commerce of the U.S. However, because these regulations are being put in place in order to further a legitimate domestic objective, namely to increase the security of the

U.S., any obstacles created by the regulation are not considered unnecessary obstacles.

Environment

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

This rulemaking will not significantly impact the coastal zone. Further, the rulemaking and the execution of this interim 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

33 CFR Part 104

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

33 CFR Part 160

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

46 CFR Part 2

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

46 CFR Part 31

Cargo vessels, Inspection and certification, Maritime security.

46 CFR Part 71

Passenger vessels, Inspection and certification, Maritime security.

46 CFR Part 91

Cargo vessels, Inspection and Certification, Maritime security.

46 CFR Part 115

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

46 CFR Part 126

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

46 CFR Part 176

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

For the reasons discussed in the preamble, the Coast Guard adds 33 CFR part 104 and amends 33 CFR part 160 and part 165, and 46 CFR parts 2, 31, 71, 91, 115, 126, and 176 as follows:

1. Add part 104 to subchapter H to read as follows:

PART 104—VESSEL SECURITY

Subpart A—General

Sec.

104.100 Definitions.

104.105 Applicability.

104.110 Exemptions.

104.115 Compliance dates.

- 104.120 Compliance documentation.
 - 104.125 Noncompliance.
 - 104.130 Waivers.
 - 104.135 Equivalents.
 - 104.140 Alternative Security Programs.
 - 104.145 Maritime Security (MARSEC) Directive.
 - 104.150 Right to appeal.
- Subpart B—Vessel Security Requirements
- Sec.
- 104.200 Owner or operator.
 - 104.205 Master.
 - 104.210 Company Security Officer (CSO).
 - 104.215 Vessel Security Officer (VSO).
 - 104.220 Company or vessel personnel with security duties.
 - 104.225 Security training for all other vessel personnel.
 - 104.230 Drill and exercise requirements.
 - 104.235 Vessel recordkeeping requirements.
 - 104.240 Maritime Security (MARSEC) Level coordination and implementation.
 - 104.245 Communications.
 - 104.250 Procedures for interfacing with facilities and other vessels.
 - 104.255 Declaration of Security (DoS).
 - 104.260 Security systems and equipment maintenance.

- 104.265 Security measures for access control.
- 104.270 Security measures for restricted areas.
- 104.275 Security measures for handling cargo.
- 104.280 Security measures for delivery of vessel stores and bunkers.
- 104.285 Security measures for monitoring.
- 104.290 Security incident procedures.
- 104.292 Additional requirements--passenger vessels and ferries.
- 104.295 Additional requirements--cruise ships.
- 104.297 Additional requirements--vessels on international voyages.
- Subpart C--Vessel Security Assessment (VSA)
Sec.
 - 104.300 General.
 - 104.305 Vessel Security Assessment (VSA) requirements.
 - 104.310 Submission requirements.
- Subpart D--Vessel Security Plan (VSP)
Sec.
 - 104.400 General.
 - 104.405 Format of the Vessel Security Plan (VSP).
 - 104.410 Submission and approval.
 - 104.415 Amendment and audit.

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.

Subpart A—General

§ 104.100 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

§ 104.105 Applicability.

(a) This part applies to the owner or operator of any:

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

(2) Foreign commercial vessel greater than 100 gross register tons not subject to SOLAS;

(3) Commercial vessel greater than 100 gross register tons subject to 46 CFR subchapter I, except commercial fishing vessels inspected under 46 CFR 105;

(4) Vessel subject to 46 CFR subchapter L;

(5) Passenger vessel subject to 46 CFR subchapters H or K;

(6) Other passenger vessel carrying more than 12 passengers that is engaged on an international voyage;

(7) Barge subject to 46 CFR subchapters D or O;

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

(9) Tankship subject to 46 CFR subchapters D or O;

and

(10) Towing vessel greater than eight meters in registered length that is engaged in towing a barge or barges subject to this part.

(b) An owner or operator of any vessel not covered in paragraph (a) of this section is subject to parts 101 through 103 of this subchapter.

(c) Foreign vessels that have on board a valid International Ship Security Certificate (ISSC) that attests to the vessel's compliance with SOLAS Chapter XI-2 and the ISPS Code, part A (Incorporated by reference, see § 101.115 of this chapter), and having taken into account the relevant provisions in the ISPS Code, part B, will be deemed to be in compliance with this part, except for §§ 104.240, 104.255, 104.292, and 104.295 as appropriate.

(d) Except pursuant to international treaty, convention, or agreement to which the U.S. is a party, this part does not apply to any foreign vessel that is not

destined for, or departing from, a port or place subject to the jurisdiction of the U.S. and that is in:

(1) Innocent passage through the territorial sea of the U.S.; or

(2) Transit through the navigable waters of the U.S. that form a part of an international strait.

§ 104.110 Exemptions.

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

§ 104.115 Compliance dates.

(a) On or before [Insert 180 days after publication in the Federal Register], each vessel owner or operator must submit to the Commanding Officer, Marine Safety Center for each vessel the Vessel Security Plan described in subpart D of this part for review and approval.

(b) On or before [Insert 365 days after publication in the Federal Register], each vessel must be operating in compliance with this part.

(c) On or before 1 July 2004, foreign vessels must carry on board a valid International Ship Security Certificate that certifies that the verifications required by Section 19.1 of part A of the ISPS Code (Incorporated by

reference, see § 101.115 of this chapter) have been completed, that the vessel meets the applicable requirements of SOLAS Chapter XI-2 (Incorporated by reference, see § 101.115 of this chapter) and the ISPS Code, part A, and that the vessel is provided with an approved security plan.

§ 104.120 Compliance documentation.

(a) Each vessel owner or operator subject to this part must ensure, no later than 1 July 2004, that copies of the following documents are carried on board the vessel and are made available to the Coast Guard upon request:

(1) The approved Vessel Security Plan (VSP) and any approved revisions or amendments thereto, and a letter of approval from the Commanding Officer, Marine Safety Center (MSC);

(2) The VSP submitted for approval and a current acknowledgement letter from the Commanding Officer, MSC, stating that the Coast Guard is currently reviewing the VSP submitted for approval, and that the vessel may continue to operate so long as the vessel remains in compliance with the submitted plan;

(3) For vessels operating under a Coast Guard-approved Alternative Security Program as provided in § 104.140, a copy of the Alternative Security Program the

vessel is using and a letter signed by the vessel owner or operator, stating which Alternative Security Program the vessel is using and certifying that the vessel is in full compliance with that program; or

(4) For foreign vessels, a valid International Ship Security Certificate that attests to the vessel's compliance with SOLAS Chapter XI-2 and the ISPS Code, part A (Incorporated by reference, see § 101.115 of this subchapter), and having taken into account the relevant provisions in the ISPS Code, part B.

(b) Each owner or operator of an unmanned vessel subject to this part must maintain the documentation described in paragraphs (a)(1), (2), or (3) of this section. The letter required by each of those paragraphs must be carried on board the vessel. The plan or program required by each of those paragraphs must not be carried on board the vessel, but must be maintained in a secure location. During scheduled inspections, the plan or program must be made available to the Coast Guard upon request.

§ 104.125 Noncompliance.

When a vessel is not in compliance with the requirements of this part, the vessel owner or operator

must notify the cognizant COTP and request a waiver to continue operations.

§ 104.130 Waivers.

Any vessel owner or operator may apply for a waiver of any requirement of this part that the owner or operator considers unnecessary in light of the nature or operating conditions of the vessel. A request for a waiver must be submitted in writing with justification to the Commandant (G-MP) at 2100 Second St., S.W., Washington, DC 20593. The Commandant (G-MP) may require the vessel owner or operator to provide additional data for determining the validity of the requested waiver. The Commandant (G-MP) may grant, in writing, a waiver with or without conditions only if the waiver will not reduce the overall security of the vessel, its passengers, its crew, or its cargo, or facilities or ports that the vessel may visit.

§ 104.135 Equivalents.

For any measure required by this part, the vessel owner or operator may propose an equivalent as provided in § 101.130 of this subchapter.

§ 104.140 Alternative Security Programs.

A vessel owner or operator may use an Alternative Security Program as approved under § 101.120 of this subchapter if:

(a) The Alternative Security Program is appropriate to that class of vessel;

(b) The vessel does not engage on international voyages; and

(c) The Alternative Security Program is implemented in its entirety.

§ 104.145 Maritime Security (MARSEC) Directive.

Each vessel owner or operator subject to this part must comply with any instructions contained in a MARSEC Directive issued under § 101.405 of this subchapter.

§ 104.150 Right to appeal.

Any person directly affected by a decision or action taken under this part, by or on behalf of the Coast Guard, may appeal as described in § 101.420 of this subchapter.

Subpart B—Vessel Security Requirements

§ 104.200 Owner or operator.

(a) Each vessel owner or operator must ensure that the vessel operates in compliance with the requirements of this part.

(b) For each vessel, the vessel owner or operator must:

(1) Define the security organizational structure for each vessel and provide all personnel exercising security

duties or responsibilities within that structure with the support needed to fulfill security obligations;

(2) Designate, in writing, by name or title, a Company Security Officer (CSO), a Vessel Security Officer (VSO) for each vessel, and identify how those officers can be contacted at any time;

(3) Ensure personnel receive training, drills, and exercises enabling them to perform their assigned security duties;

(4) Ensure vessel security records are kept;

(5) Ensure that adequate coordination of security issues takes place between vessels and facilities; this includes the execution of a Declaration of Security (DoS);

(6) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility of visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with facility operators in advance of a vessel's arrival;

(7) Ensure security communication is readily available;

(8) Ensure coordination with and implementation of changes in Maritime Security (MARSEC) Level;

- (9) Ensure that security systems and equipment are installed and maintained;
- (10) Ensure that vessel access, including the embarkation of persons and their effects, are controlled;
- (11) Ensure that restricted areas are controlled;
- (12) Ensure that cargo and vessel stores and bunkers are handled in compliance with this part;
- (13) Ensure restricted areas, deck areas, and areas surrounding the vessel are monitored;
- (14) Provide the Master, or for vessels on domestic routes only, the CSO, with the following information:
- (i) Parties responsible for appointing vessel personnel, such as vessel management companies, manning agents, contractor, concessionaires (for example, retail sales outlets, casinos, etc.);
 - (ii) Parties responsible for deciding the employment of the vessel, including time or bareboat charters or any other entity acting in such capacity; and
 - (iii) In cases when the vessel is employed under the terms of a charter party, the contract details of those documents, including time or voyage charters; and
- (15) Give particular consideration to the convenience, comfort, and personal privacy of vessel

personnel and their ability to maintain their effectiveness over long periods.

§ 104.205 Master.

(a) Nothing in this part is intended to permit the Master to be constrained by the Company, the vessel owner or operator, or any other person, from taking or executing any decision which, in the professional judgment of the Master, is necessary to maintain the safety and security of the vessel. This includes denial of access to persons—except those identified as duly authorized by the cognizant government authority—or their effects, and refusal to load cargo, including containers or other closed cargo transport units.

(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 seem best under all circumstances. In such cases:

(1) The Master must, as soon as practicable, inform the nearest COTP. If the vessel is on a foreign voyage, the Master must promptly inform the Coast Guard at 1-800-424-8802, direct telephone at 202-267-2675, fax at 202-267-

2165, TDD at 202-267-4477, or Email at 1st-nrcinfo@comdt.uscg.mil and if subject to the jurisdiction of a foreign government, the relevant maritime authority of that foreign government;

(2) The temporary security measures must, to the highest possible degree, be commensurate with the prevailing Maritime Security (MARSEC) Level; and

(3) The owner or operator must ensure that such conflicts are resolved to the satisfaction of the cognizant COTP, or for vessels on international voyages, the Commandant (G-MP), and that the possibility of recurrence is minimized.

§ 104.210 Company Security Officer (CSO).

(a) General.--

(1) Each vessel owner or operator must designate in writing a CSO.

(2) A vessel owner or operator may designate a single CSO for all its vessels to which this part applies, or may designate more than one CSO, in which case the owner or operator must clearly identify the vessels for which each CSO is responsible.

(3) A CSO may perform other duties within the owner or operator's organization, provided he or she is able to perform the duties and responsibilities required of a CSO.

(4) The CSO may delegate duties required by this part, but remains responsible for the performance of those duties.

(b) Qualifications.--

(1) The CSO must have general knowledge, through training or equivalent job experience, in the following:

(i) Security administration and organization of the company's vessel(s);

(ii) Vessel, facility, and port operations relevant to that industry;

(iii) Vessel and facility security measures, including the meaning and the consequential requirements of the different Maritime Security (MARSEC) Levels;

(iv) Emergency preparedness and response and contingency planning;

(v) Security equipment and systems and their operational limitations;

(vi) Methods of conducting audits, inspection and control and monitoring techniques; and

(vii) Techniques for security training and education, including security measures and procedures.

(2) In addition to knowledge and training in paragraph (b)(1) of this section, the CSO must have general

knowledge through training or equivalent job experience in the following, as appropriate:

- (i) Relevant international conventions, codes, and recommendations;
- (ii) Relevant government legislation and regulations;
- (iii) Responsibilities and functions of other security organizations;
- (iv) Methodology of Vessel Security Assessment;
- (v) Methods of vessel security surveys and inspections;
- (vi) Instruction techniques for security training and education, including security measures and procedures;
- (vii) Handling sensitive security information and security related communications;
- (viii) Knowledge of current security threats and patterns;
- (ix) Recognition and detection of dangerous substances and devices;
- (x) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
- (xi) Techniques used to circumvent security measures;
- (xii) Methods of physical screening and non-intrusive inspections;

(xiii) Security drills and exercises, including drills and exercises with facilities; and

(xiv) Assessment of security drills and exercises.

(c) Responsibilities. In addition to those responsibilities and duties specified elsewhere in this part, the CSO must, for each vessel for which he or she has been designated:

(1) Keep the vessel apprised of potential threats or other information relevant to its security;

(2) Ensure a Vessel Security Assessment (VSA) is carried out;

(3) Ensure a Vessel Security Plan (VSP) is developed, approved, and maintained;

(4) Ensure the VSP is modified when necessary;

(5) Ensure vessel security activities are audited;

(6) Arrange for Coast Guard inspections under 46 CFR part 2;

(7) Ensure the timely or prompt correction of problems identified by audits or inspections;

(8) Enhance security awareness and vigilance within the owner's or operator's organization;

(9) Ensure relevant personnel receive adequate security training;

(10) Ensure communication and cooperation between the vessel and the port and facilities with which the vessel interfaces;

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

(12) Ensure that when sister-vessel or fleet security plans are used, the plan for each vessel reflects the vessel-specific information accurately;

(13) Ensure compliance with an Alternative Security Program or equivalents approved under this subchapter, if appropriate; and

(14) Ensure security measures give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods.

§ 104.215 Vessel Security Officer (VSO).

(a) General.

(1) A VSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and responsibilities required of the VSO for each such vessel.

(2) For manned vessels, the VSO must be a member of the crew.

(3) For unmanned vessels, the same person may serve as the VSO for more one than one unmanned vessel. If a person serves as the VSO for more than one unmanned vessel,

the name of each unmanned vessel for which he or she is the VSO must be listed in the Vessel Security Plan (VSP).

(4) The VSO of any unmanned barge and the VSO of any towing vessel interfacing with the barge must coordinate and ensure the implementation of security measures applicable to both vessels during the period of their interface.

(5) The VSO may assign security duties to other vessel personnel; however, the VSO remains responsible for these duties.

(b) Qualifications. The VSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Those items listed in § 104.210 (b) (1) and (b) (2) of this part;

(2) Vessel layout;

(3) The VSP and related procedures, including scenario-based response training;

(4) Crowd management and control techniques;

(5) Operations of security equipment and systems; and

(6) Testing and calibration of security equipment and systems, and their maintenance while at sea.

(c) Responsibilities. In addition to those responsibilities and duties specified elsewhere in this

part, the VSO must, for each vessel for which he or she has been designated:

- (1) Regularly inspect the vessel to ensure that security measures are maintained;
- (2) Ensure maintenance and supervision of the implementation of the VSP, and any amendments to the VSP;
- (3) Ensure the coordination and handling of cargo and vessel stores and bunkers in compliance with this part;
- (4) Propose modifications to the VSP to the Company Security Officer (CSO);
- (5) Ensure that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions;
- (6) Ensure security awareness and vigilance on board the vessel;
- (7) Ensure adequate security training for vessel personnel;
- (8) Ensure the reporting and recording of all security incidents;
- (9) Ensure the coordinated implementation of the VSP with the CSO and the relevant Facility Security Officer, when applicable;
- (10) Ensure security equipment is properly operated, tested, calibrated and maintained; and

(11) Ensure consistency between security requirements and the proper treatment of vessel personnel affected by those requirements.

§ 104.220 Company or vessel personnel with security duties.

Company and vessel personnel responsible for security duties must have knowledge, through training or equivalent job experience, in the following, as appropriate:

- (a) Knowledge of current security threats and patterns;
- (b) Recognition and detection of dangerous substances and devices;
- (c) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
- (d) Techniques used to circumvent security measures;
- (e) Crowd management and control techniques;
- (f) Security related communications;
- (g) Knowledge of emergency procedures and contingency plans;
- (h) Operation of security equipment and systems;
- (i) Testing and calibration of security equipment and systems, and their maintenance while at sea;
- (j) Inspection, control, and monitoring techniques;

(k) Relevant provisions of the Vessel Security Plan (VSP);

(l) Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores; and

(m) The meaning and the consequential requirements of the different Maritime Security (MARSEC) Levels.

§ 104.225 Security training for all other vessel personnel.

All other vessel personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge of, through training or equivalent job experience in the following:

(a) Relevant provisions of the Vessel Security Plan (VSP);

(b) The meaning and the consequential requirements of the different Maritime Security (MARSEC) Levels, including emergency procedures and contingency plans;

(c) Recognition and detection of dangerous substances and devices;

(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

(e) Techniques used to circumvent security measures.

§ 104.230 Drill and exercise requirements.

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

(b) Drills.--

(1) The VSO must ensure that at least one security drill is conducted at least every three months, except when a vessel is out of service due to repairs or seasonal suspension of operation provided that in such cases a drill must be conducted within one week of the vessel's reactivation. Security drills may be held in conjunction with non-security drills where appropriate.

(2) Drills must test individual elements of the VSP, including response to security threats and incidents. Drills should take into account the types of operations of the vessel, vessel personnel changes, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.

(3) If the vessel is moored at a facility on the date the facility has planned to conduct any drills, the vessel may, but is not required to, participate in the facility's scheduled drill.

(4) Drills must be conducted within one week whenever the percentage of vessel personnel with no prior participation in a vessel security drill on that vessel exceeds 25 percent.

(c) Exercises.--

(1) Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be:

(i) Full scale or live;

(ii) Tabletop simulation or seminar;

(iii) Combined with other appropriate exercises; or

(iv) A combination of the elements in paragraphs

(c)(2)(i) through (iii) of this section.

(3) Exercises may be vessel-specific or part of a cooperative exercise program to exercise applicable facility and vessel security plans or comprehensive port exercises.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the security program and must include the substantial and active participation of relevant company and vessel security personnel, and may include facility security personnel and government authorities depending on the scope and the nature of the exercises.

§ 104.235 Vessel recordkeeping requirements.

(a) Unless otherwise specified in this section, the Vessel Security Officer must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized deletion, destruction, or amendment. The following records must be kept:

(1) Training. For each security training session, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) Drills and exercises. For each drill or exercise, the date held, description of drill or exercise, list of participants; and any best practices or lessons learned which may improve the Vessel Security Plan (VSP);

(3) Incidents and breaches of security. Date and time of occurrence, location within the port, location within the vessel, description of incident or breaches, to whom it was reported, and description of the response;

(4) Changes in Maritime Security (MARSEC) Levels. Date and time of notification received, and time of compliance with additional requirements;

(5) Maintenance, calibration, and testing of security equipment. For each occurrence of maintenance, calibration, and testing, the date and time, and the specific security equipment involved;

(6) Security threats. Date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported, and description of the response;

(7) Declaration of Security (DoS). Manned vessels must keep on board a copy of the last 10 DoSs and a copy of each continuing DoS for at least 90 days after the end of its effective period; and

(8) Annual audit of the VSP. For each annual audit, a letter certified by the VSO stating the date the audit was completed.

(c) Any records required by this part must be protected from unauthorized access or disclosure.

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

(a) The vessel owner or operator must ensure that, prior to entering a port, all measures are taken that are specified in the Vessel Security Plan (VSP) for compliance with the MARSEC Level in effect for the port.

(b) When notified of an increase in the MARSEC Level, the vessel owner or operator must ensure:

(1) If a higher MARSEC Level is set for the port in which the vessel is located or is about to enter, the vessel complies, without undue delay, with all measures specified in the VSP for compliance with that higher MARSEC Level;

(2) The COTP is notified as required by § 101.300(c) when compliance with the higher MARSEC Level has been implemented; and

(3) For vessels in port, that compliance with the higher MARSEC Level has taken place within 12 hours of the notification.

(c) For MARSEC Levels 2 and 3, the Vessel Security Officer must brief all vessel personnel of identified threats, emphasize reporting procedures, and stress the need for increased vigilance.

(d) An owner or operator whose vessel is not in compliance with the requirements of this section must inform the COTP and obtain approval prior to entering any port, prior to interfacing with another vessel or with a facility or to continuing operations.

(e) For MARSEC Level 3, in addition to the requirements in this part, a vessel owner or operator may be required to implement additional measures, pursuant to 33 CFR part 6, 160 or 165, as appropriate, which may include but are not limited to:

(1) Arrangements to ensure that the vessel can be towed or moved if deemed necessary by the Coast Guard;

(2) Use of waterborne security patrol;

(3) Use of armed security personnel to control access to the vessel and to deter, to the maximum extent practical, a TSI; or

(4) Screening the vessel for the presence of dangerous substances and devices underwater or other threats.

§ 104.245 Communications.

(a) The Vessel Security Officer must have a means to effectively notify vessel personnel of changes in security conditions on board the vessel.

(b) Communications systems and procedures must allow effective and continuous communication between the vessel security personnel, facilities interfacing with the vessel, vessels interfacing with the vessel, and national or local authorities with security responsibilities.

(c) Communication systems and procedures must enable vessel personnel to notify, in a timely manner, shore side authorities or other vessels of a security threat or incident on board.

§ 104.250 Procedures for interfacing with facilities and other vessels.

(a) The vessel owner or operator must ensure that there are measures for interfacing with facilities and other vessels at all MARSEC Levels.

(b) For each U.S. flag vessel that calls on foreign ports or facilities, the vessel owner or operator must ensure procedures for interfacing with those ports and facilities are established.

§ 104.255 Declaration of Security (DoS).

(a) Each vessel owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from a facility or other vessel.

(b) At MARSEC Level 1, the Master or Vessel Security Officer (VSO), or their designated representative, of any cruise ship or manned vessel carrying Certain Dangerous Cargoes, in bulk, must complete and sign a DoS with the VSO or Facility Security Officer (FSO), or their designated representative, of any vessel or facility with which it interfaces.

(1) For a vessel-to-facility interface, prior to arrival of a vessel to a facility, the FSO and Master, VSO, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility. Upon a vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the FSO or Master, VSO, or designated representatives must sign the written DoS.

(2) For a vessel engaging in a vessel-to-vessel interface, prior to the interface, the respective Masters, VSOs, or their designated representatives must coordinate security needs and procedures, and agree upon the contents

of the DoS for the period of time the vessel is at the facility. Upon the vessel-to-vessel interface and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, VSOs, or designated representatives must sign the written DoS.

(c) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any vessel required to comply with this part must sign and implement a DoS prior to any vessel-to-vessel interface.

(d) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any vessel required to comply with this part must sign and implement a DoS with the FSO of any facility on which it calls prior to any cargo transfer operation or passenger embarkation or disembarkation.

(e) At MARSEC Levels 1 and 2, VSOs of vessels that frequently interface with the same facility may implement a continuing DoS for multiple visits, provided that:

- (1) The DoS is valid for the specific MARSEC Level;
- (2) The effective period at MARSEC Level 1 does not exceed 90 days; and
- (3) The effective period at MARSEC Level 2 does not exceed 30 days.

(f) When the MARSEC Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS must be signed and implemented in accordance with this section.

(g) The COTP may require at any time, at any MARSEC Level, any manned vessel subject to this part to implement a DoS with the VSO or FSO prior to any vessel-to-vessel or vessel-to-facility interface when he or she deems it necessary.

§ 104.260 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated and maintained according to the manufacturer's recommendation.

(b) The results of testing completed under paragraph (a) of this section shall be recorded in accordance with § 104.235. Any deficiencies shall be promptly corrected.

(c) The Vessel Security Plan (VSP) must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 104.265 Security measures for access control.

(a) General. The vessel owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on board; and

(3) Control access to the vessel.

(b) The vessel owner or operator must ensure that:

(1) The locations providing means of access to the vessel where access restrictions or prohibitions are applied for each Maritime Security (MARSEC) Level to prevent unauthorized access. "Means of access" include, but are not limited, to all:

(i) Access ladders;

(ii) Access gangways;

(iii) Access ramps;

(iv) Access doors, side scuttles, windows, and ports;

(v) Mooring lines and anchor chains; and

(vi) Cranes and hoisting gear;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them; and

(3) The means of identification required to allow individuals to access the vessel and remain on the vessel without challenge are established.

(c) The vessel owner or operator must ensure that an identification system is established for checking the identification of vessel personnel or other persons seeking access to the vessel that:

(1) Allows identification of authorized and unauthorized persons at any MARSEC Level;

(2) Is coordinated, when practicable, with identification systems at facilities used by the vessel;

(3) Is updated regularly;

(4) Uses disciplinary measures to discourage abuse;

(5) Allows temporary or continuing access for vessel personnel and visitors, including seafarer's chaplains and union representatives, through the use of a badge or other system to verify their identity; and

(6) Allow certain long-term, frequent vendor representatives to be treated more as employees than as visitors.

(d) The vessel owner or operator must establish in the approved Vessel Security Plan (VSP) the frequency of application of any security measures for access control, particularly if these security measures are applied on a random or occasional basis.

(e) MARSEC Level 1. The vessel owner or operator must ensure security measures in this paragraph are implemented to:

(1) Screen persons, baggage (including carry-on items), personal effects, and vehicles for dangerous substances and devices at the rate specified in the approved Vessels Security Plan (VSP);

(2) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Boarding the vessel is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to board;

(3) Check the identification of any person seeking to board the vessel, including vessel passengers and crew, facility employees, vendors, personnel duly authorized by the cognizant government authorities, and visitors. This check includes confirming the reason for boarding by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system required in paragraph (c) of this section;

(4) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of vessel personnel, to establish his or her identity or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(5) Deter unauthorized access to the vessel;

(6) Identify access points that must be secured or attended to deter unauthorized access;

(7) Lock or otherwise prevent access to unattended spaces that adjoin areas to which passengers and visitors have access;

(8) Provide a designated secure area on board or in liaison with a facility, for conducting inspections and screening of people, baggage (including carry-on items), personal effects, vehicles and the vehicle's contents;

(9) Ensure vessel personnel are not required to engage in or be subjected to screening, of the person or of personal effects, by other vessel personnel, unless security clearly requires it. Any such screening must be

conducted in a way that takes into full account individual human rights and preserves the individual's basic human dignity;

(10) Ensure the screening of all unaccompanied baggage;

(11) Ensure checked persons and their personal effects are segregated from unchecked persons and their personal effects;

(12) Ensure embarking passengers are segregated from disembarking passengers;

(13) Ensure, in liaison with the facility, a defined percentage of vehicles to be loaded aboard passenger vessels are screened prior to loading at the rate specified in the approved VSP;

(14) Ensure, in liaison with the facility, all unaccompanied vehicles to be loaded on passenger vessels are screened prior to loading; and

(15) Respond to the presence of unauthorized persons on board, including repelling unauthorized boarders.

(f) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures,

as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(1) Increasing the frequency and detail of screening of people, personal effects, and vehicles being embarked or loaded onto the vessel as specified for MARSEC Level 2 in the approved VSP;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to patrol deck areas during periods of reduced vessel operations to deter unauthorized access;

(4) Limiting the number of access points to the vessel by closing and securing some access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the vessel, which may include, in liaison with the facility, providing boat patrols; and

(7) Establishing a restricted area on the shoreside of the vessel, in close cooperation with the facility.

(g) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC

Level 3 in the approved VSP. The additional security measures may include:

(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied baggage more extensively, for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage on board;

(3) Being prepared to cooperate with responders and facilities;

(4) Limiting access to the vessel to a single, controlled access point;

(5) Granting access to only those responding to the security incident or threat thereof;

(6) Suspending embarkation and/or disembarkation of personnel;

(7) Suspending cargo operations;

(8) Evacuating the vessel;

(9) Moving the vessel; and

(10) Preparing for a full or partial search of the vessel.

§ 104.270 Security measures for restricted areas.

(a) General. The vessel owner or operator must ensure the designation of restricted areas in order to:

- (1) Prevent or deter unauthorized access;
- (2) Protect persons authorized to be on board;
- (3) Protect the vessel;
- (4) Protect sensitive security areas within the vessel;
- (5) Protect security and surveillance equipment and systems; and
- (6) Protect cargo and vessel stores from tampering.

(b) Designation of Restricted Areas. The vessel owner or operator must ensure restricted areas are designated on board the vessel, as specified in the approved plan. Restricted areas must include, as appropriate:

- (1) Navigation bridge, machinery spaces and other control stations;
- (2) Spaces containing security and surveillance equipment and systems and their controls and lighting system controls;

(3) Ventilation and air-conditioning systems and other similar spaces;

(4) Spaces with access to potable water tanks, pumps, or manifolds;

(5) Spaces containing dangerous goods or hazardous substances;

(6) Spaces containing cargo pumps and their controls;

(7) Cargo spaces and spaces containing vessel stores;

(8) Crew accommodations; and

(9) Any other spaces or areas vital to the security of the vessel.

(c) The vessel owner or operator must ensure that security measures and policies are established to:

(1) Identify which vessel personnel are authorized to have access;

(2) Determine which persons other than vessel personnel are authorized to have access;

(3) Determine the conditions under which that access may take place;

(4) Define the extent of any restricted area;

(5) Define the times when access restrictions apply;

and

(6) Clearly mark all restricted areas and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

(d) Maritime Security (MARSEC) Level 1. The vessel owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

- (1) Locking or securing access points;
- (2) Monitoring and using surveillance equipment;
- (3) Using guards or patrols; and
- (4) Using automatic intrusion detection devices, which if used must activate an audible and/or visual alarm at a location that is continuously attended or monitored, to alert vessel personnel to unauthorized access.

(e) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

- (1) Increasing the frequency and intensity of monitoring and access controls on existing restricted access areas;

(2) Restricting access to areas adjacent to access points;

(3) Providing continuous monitoring of each area, using surveillance equipment; and

(4) Dedicating additional personnel to guard or patrol each area.

(f) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may include:

(1) Restricting access to additional areas; and

(2) Searching restricted areas as part of a security sweep of the vessel.

§ 104.275 Security measures for handling cargo.

(a) General. The vessel owner or operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the facility, are specified in order to:

(1) Deter tampering;

(2) Prevent cargo that is not meant for carriage from being accepted and stored on board the vessel;

(3) Identify cargo that is approved for loading onto the vessel;

(4) Include inventory control procedures at access points to the vessel;

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

(6) Be able to check cargo for dangerous substances and devices at the rate specified in the approved Vessel Security Plan. Means to check cargo include:

(i) Visual examination;

(ii) Physical examination;

(iii) Detection devices such as scanners; or

(iv) Canines.

(b) Maritime Security (MARSEC) Level 1. At MARSEC Level 1, the vessel owner or operator must ensure the implementation of measures to:

(1) Routinely check cargo and cargo spaces prior to and during cargo handling;

(2) Check that cargo to be loaded matches the cargo documentation, or that cargo markings or container numbers match the information provided with shipping documents;

(3) Ensure, in liaison with the facility, that vehicles to be loaded on board car carriers, RO-RO, and

passenger ships are subjected to screening prior to loading, in accordance with the frequency required in the VSP; and

(4) Check, in liaison with the facility, seals or other methods used to prevent tampering.

(c) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved Vessel Security Plan (VSP). These additional security measures may include:

(1) Increasing the frequency and detail of checking cargo and cargo spaces;

(2) Intensifying checks to ensure that only the intended cargo, container, or other cargo transport units are loaded;

(3) Intensifying screening of vehicles to be loaded on car-carriers, RO-RO, and passenger vessels;

(4) In liaison with the facility, increasing frequency and detail in checking seals or other methods used to prevent tampering;

(5) Increasing the frequency of the use of scanning/detection equipment, mechanical devices, or canines; or

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

(d) MARSEC Level 3. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may include:

(1) Suspending loading or unloading of cargo;

(2) Being prepared to cooperate with responders and facilities; or

(3) Verifying the inventory and location of any hazardous materials carried on board.

§ 104.280 Security measures for delivery of vessel stores and bunkers.

(a) General. The vessel owner or operator must ensure that security measures relating to the delivery of vessel stores and bunkers are implemented to:

(1) Check vessel stores for package integrity;

(2) Prevent vessel stores from being accepted without inspection;

(3) Deter tampering; and

(4) Prevent vessel stores and bunkers from being accepted unless ordered. For vessels that routinely use a facility, a vessel owner or operator may establish and implement standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation.

(b) Maritime Security (MARSEC) Level 1. At MARSEC Level 1, the vessel owner or operator must ensure the implementation of measures to:

(1) Check vessel stores before being accepted;

(2) Check that vessel stores and bunkers match the order prior to being brought on board or being bunkered; and

(3) Ensure that vessel stores are controlled or immediately and securely stowed following delivery.

(c) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved Vessel

Security Plan (VSP). These additional security measures may include:

(1) Intensifying inspection of the vessel stores during delivery; or

(2) Checking vessel stores prior to receiving them on board.

(d) MARSEC Level 3. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may include:

(1) Checking all vessel stores more extensively;

(2) Restricting or suspending delivery of vessel stores and bunkers; or

(3) Refusing to accept vessel stores on board.

§ 104.285 Security measures for monitoring.

(a) General.--

(1) The vessel owner or operator must ensure the implementation of security measures and have the capability to continuously monitor, through a combination of lighting, watchkeepers, security guards, deck watches, waterborne patrols and automatic intrusion-detection devices, or

surveillance equipment, as specified in their approved Vessel Security Plan (VSP), the--

- (i) Vessel;
- (ii) Restricted areas on board the vessel; and
- (iii) Area surrounding the vessel.

(2) The following must be considered when establishing the appropriate level and location of lighting:

(i) Vessel personnel should be able to detect activities on and around the vessel, on both the shore side and the waterside;

(ii) Coverage should facilitate personnel identification at access points;

(iii) Coverage may be provided through coordination with the port or facility; and

(iv) Lighting effects, such as glare, and its impact on safety, navigation, and other security activities.

(b) Maritime Security (MARSEC) Level 1. At MARSEC Level 1, the vessel owner or operator must ensure the implementation of security measures, which may be done in coordination with a facility, to:

(1) Monitor the vessel, particularly vessel access points and restricted areas;

(2) Be able to conduct emergency searches of the vessel;

(3) Ensure that equipment or system failures or malfunctions are identified and corrected;

(4) Ensure that any automatic intrusion detection device sets off an audible or visual alarm, or both, at a location that is continually attended or monitored;

(5) Light deck and vessel access points during the period between sunset and sunrise and periods of limited visibility sufficiently to allow visual identification of persons seeking access to the vessel; and

(6) Use maximum available lighting while underway, during the period between sunset and sunrise, consistent with safety and international regulations.

(c) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(1) Increasing the frequency and detail of security patrols;

(2) Increasing the coverage and intensity of lighting, alone or in coordination with the facility;

(3) Using or increasing the use of security and surveillance equipment;

(4) Assigning additional personnel as security lookouts;

(5) Coordinating with boat patrols, when provided; or

(6) Coordinating with shoreside foot or vehicle patrols, when provided.

(d) MARSEC Level 3. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. These additional security measures may include:

(1) Cooperating with responders and facilities;

(2) Switching on all lights;

(3) Illuminating the vicinity of the vessel;

(4) Switching on all surveillance equipment capable of recording activities on, or in the vicinity of, the vessel;

(5) Maximizing the length of time such surveillance equipment can continue to record;

(6) Preparing for underwater inspection of the hull;

and

(7) Initiating measures, including the slow revolution of the vessel's propellers, if practicable, to deter underwater access to the hull of the vessel.

§ 104.290 Security incident procedures.

For each Maritime Security (MARSEC) Level, the vessel owner or operator must ensure the Vessel Security Officer (VSO) and vessel security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical vessel and vessel-to-facility interface operations, to include:

- (1) Prohibiting entry into affected area;
- (2) Denying access to the vessel, except to those responding to the emergency;
- (3) Implementing MARSEC Level 3 security measures throughout the vessel;
- (4) Stopping cargo-handling operations; and
- (5) Notifying shoreside authorities or other vessels of the emergency;

(b) Evacuating the vessel in case of security threats or breaches of security;

(c) Reporting security incidents as required in § 101.305;

(d) Briefing all vessel personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

(e) Securing non-critical operations in order to focus response on critical operations.

§ 104.292 Additional requirements--passenger vessels and ferries.

(a) At all Maritime Security (MARSEC) Levels, the vessel owner or operator must ensure security sweeps are performed, prior to getting underway, after any period the vessel was unattended.

(b) As an alternative to the identification checks and passenger screening requirements in § 104.265 (e) (1), (e) (3), and (e) (8), the owner or operator of a passenger vessel or ferry may ensure security measures are implemented that include:

(1) Searching selected areas prior to embarking passengers and prior to sailing; and

(2) Implementing one or more of the following:

(i) Performing routine security patrols;

(ii) Providing additional closed-circuit television to monitor passenger areas; or

(iii) Securing all non-passenger areas.

(c) Passenger vessels certificated to carry more than 2000 passengers, working in coordination with the terminal, may be subject to additional vehicle screening requirements in accordance with a MARSEC Directive or other orders issued by the Coast Guard.

(d) At MARSEC Level 2, a vessel owner or operator must ensure, in addition to MARSEC Level 1 measures, the implementation of the following:

(1) Search selected areas prior to embarking passengers and prior to sailing;

(2) Passenger vessels certificated to carry less than 2000 passengers, working in coordination with the terminal, may be subject to additional vehicle screening requirements in accordance with a MARSEC Directive or other orders issued by the Coast Guard; and

(3) As an alternative to the identification and screening requirements in § 104.265(e)(3), intensify patrols, security sweeps and monitoring identified in paragraph (b) of this section.

(e) At MARSEC Level 3, a vessel owner or operator may, in addition to MARSEC Levels 1 and 2 measures, as an alternative to the identification checks and passenger screening requirements in § 104.265(e)(3), ensure that

random armed security patrols are conducted, which need not consist of vessel personnel.

§ 104.295 Additional requirements--cruise ships.

(a) At all MARSEC Levels, the owner or operator of a cruise ship must ensure the following:

(1) Screen all persons, baggage, and personal effects for dangerous substances and devices;

(2) Check the identification of all persons seeking to board the vessel; this check includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, government identification or visitor badges, or work orders;

(3) Perform security patrols; and

(4) Search selected areas prior to embarking passengers and prior to sailing.

(b) At MARSEC Level 3, the owner or operator of a cruise ship must ensure that security briefs to passengers about the specific threat are provided.

§ 104.297 Additional requirements--vessels on international voyages.

(a) An owner or operator of a U.S. flag vessel, which is subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), must be in compliance with the applicable requirements of SOLAS Chapter XI-1, SOLAS

Chapter XI-2 and the ISPS Code, part A (Incorporated by reference, see § 101.115 of this subchapter).

(b) Owners or operators of U.S. flag vessels that are required to comply with SOLAS, must ensure an International Ship Security Certificate (ISSC) as provided in 46 CFR § 2.01-25 is obtained for the vessel. This certificate must be issued by the Coast Guard.

(c) Owners or operators of vessels that require an ISSC in paragraph (b) of this section must request an inspection in writing, at least 30 days prior to the desired inspection date to the Officer in Charge, Marine Inspection for the Marine Inspection Office or Marine Safety Office of the port where the vessel will be inspected to verify compliance with this part and applicable SOLAS requirements. The inspection must be completed and the initial ISSC must be issued prior to July 1, 2004.

Subpart C—Vessel Security Assessment (VSA)

§ 104.300 General.

(a) The Vessel Security Assessment (VSA) is a written document that is based on the collection of background information and the completion and analysis of an on-scene survey.

(b) A single VSA may be performed and applied to more than one vessel to the extent that they share physical characteristics and operations.

(c) Third parties may be used in any aspect of the VSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a VSA should be able to draw upon expert assistance in the following areas:

(1) Knowledge of current security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Techniques used to circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on vessel structures and equipment;

(7) Vessel security requirements;

(8) Vessel-to-vessel and vessel-to-facility interface business practices;

(9) Contingency planning, emergency preparedness and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine engineering; and

(13) Vessel and port operations.

§ 104.305 Vessel Security Assessment (VSA) requirements.

(a) Background. The vessel owner or operator must ensure that the following background information is provided to the person or persons who will conduct the on-scene survey and assessment:

(1) General layout of the vessel, including the location of:

(i) Each actual or potential point of access to the vessel and its function;

(ii) Spaces that should have restricted access;

(iii) Essential maintenance equipment;

(iv) Cargo spaces and storage;

(v) Storage of unaccompanied baggage; and

(vi) Vessel stores;

(2) Threat assessments, including the purpose and methodology of the assessment, for the area or areas in which the vessel operates or at which passengers embark or disembark;

(3) The previous VSA, if any;

- (4) Emergency and stand-by equipment available to maintain essential services;
 - (5) Number of vessel personnel and any existing security duties to which they are assigned;
 - (6) Existing personnel training requirement practices of the vessel;
 - (7) Existing security and safety equipment for the protection of personnel, visitors, passengers, and vessels personnel;
 - (8) Escape and evacuation routes and assembly stations that have to be maintained to ensure the orderly and safe emergency evacuation of the vessel;
 - (9) Existing agreements with private security companies providing waterside or vessel security services; and
 - (10) Existing security measures and procedures, including:
 - (i) Inspection and control procedures;
 - (ii) Identification systems;
 - (iii) Surveillance and monitoring equipment;
 - (iv) Personnel identification documents;
 - (v) Communication systems;
 - (vi) Alarms;
 - (vii) Lighting;
 - (viii) Access control systems; and
 - (ix) Other security systems.
- (b) On-scene survey. The vessel owner or operator

must ensure that an on-scene survey of each vessel is

conducted. The on-scene survey is to verify or collect information required in paragraph (a) of this section. It consists of an actual survey that examines and evaluates existing vessel protective measures, procedures, and operations for:

- (1) Ensuring performance of all security duties;
- (2) Controlling access to the vessel, through the use of identification systems or otherwise;
- (3) Controlling the embarkation of vessel personnel and other persons and their effects, including personal effects and baggage whether accompanied or unaccompanied;
- (4) Supervising the handling of cargo and the delivery of vessel stores;
- (5) Monitoring restricted areas to ensure that only authorized persons have access;
- (6) Monitoring deck areas and areas surrounding the vessel; and
- (7) The ready availability of security communications, information, and equipment.

(c) Analysis and recommendations. In conducting the VSA, the Company Security Officer (CSO) must analyze the vessel background information and the on-scene survey, and while considering the requirements of this part, provide recommendations for the security measures the vessel should

include in the Vessel Security Plan (VSP). This includes but is not limited to the following:

- (1) Restricted areas;
- (2) Response procedures for fire or other emergency conditions;
- (3) Security supervision of vessel personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;
- (4) Frequency and effectiveness of security patrols;
- (5) Access control systems, including identification systems;
- (6) Security communication systems and procedures;
- (7) Security doors, barriers, and lighting;
- (8) Any security and surveillance equipment and systems;
- (9) Possible security threats, including but not limited to:
 - (i) Damage to or destruction of the vessel or an interfacing facility or vessel by dangerous substances and devices, arson, sabotage, or vandalism;
 - (ii) Hijacking or seizure of the vessel or of persons on board;
 - (iii) Tampering with cargo, essential vessel equipment or systems, or vessel stores;

(iv) Unauthorized access or use, including presence of stowaways;

(v) Smuggling dangerous substances and devices;

(vi) Use of the vessel to carry those intending to cause a security incident and/or their equipment;

(vii) Use of the vessel itself as a weapon or as a means to cause damage or destruction;

(viii) Attacks from seaward while at berth or at anchor; and

(ix) Attacks while at sea; and

(10) Evaluating the potential of each identified point of access, including open weather decks, for use by individuals who might seek to breach security, whether or not those individuals legitimately have access to the vessel.

(d) VSA report.--

(1) The vessel owner or operator must ensure that a written VSA report is prepared and included as part of the VSP. The VSA report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) Existing security measures, procedures, and operations;

- (iii) A description of each vulnerability found during the assessment;
- (iv) A description of security countermeasures that could be used to address each vulnerability;
- (v) A list of the key vessel operations that are important to protect;
- (vi) The likelihood of possible threats to key vessel operations; and
- (vii) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the vessel.

(2) The VSA report must address the following elements on board or within the vessel:

- (i) Physical security;
- (ii) Structural integrity;
- (iii) Personnel protection systems;
- (iv) Procedural policies;
- (v) Radio and telecommunication systems, including computer systems and networks; and
- (vi) Other areas that may, if damaged or used illicitly, pose a risk to people, property, or operations on board the vessel or within a facility.

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

(i) Vessel personnel;

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

(iii) Capacity to maintain safe navigation and emergency response;

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

(v) Vessel stores;

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

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

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

(i) Conflicts between safety and security measures;

(ii) Conflicts between vessel duties and security assignments;

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

(iv) Security training deficiencies; and

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

(5) The VSA must discuss and evaluate key vessel measures and operations, including:

(i) Ensuring performance of all security duties;

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

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

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

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

(vi) Monitoring deck areas and areas surrounding the vessel; and

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

(6) The VSA must be documented and the VSA report retained by the vessel owner or operator with the VSP. The VSA and VSP must be protected from unauthorized access or disclosure.

§§ 104.310 Submission requirements.

(a) A completed Vessel Security Assessment (VSA) report must be submitted with the Vessel Security Plan (VSP) required in § 104.410 of this part.

(b) A vessel owner or operator may generate and submit a report that contains the VSA for more than one vessel subject to this part, to the extent that they share similarities in physical characteristics and operations.

Subpart D—Vessel Security Plan (VSP)

§ 104.400 General.

(a) The Company Security Officer (CSO) must ensure a Vessel Security Plan (VSP) is developed and implemented for each vessel. The VSP:

(1) Must identify the CSO and VSO by name or position and provide 24-hour contact information;

(2) Must be written in English;

(3) Must address each vulnerability identified in the Vessel Security Assessment (VSA);

(4) Must describe security measures for each MARSEC Level;

(5) Must state the Master's authority as described in § 104.205; and

(6) May cover more than one vessel to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the Commanding Officer, Marine Safety Center.

(b) Except for foreign vessels that have on board a valid International Ship Security Certificate (ISSC) that

attests to the vessel's compliance with SOLAS Chapter XI-2 and the ISPS Code, part A (Incorporated by reference, see § 101.115 of this subchapter), and having taken into account the relevant provisions in the ISPS Code, part B, the VSP must be submitted for approval to the Commanding Officer, Marine Safety Center (MSC), 400 Seventh Street, SW, Room 6302, Nassif Building, Washington, DC 20590-0001, in a written or electronic format. Format for submitting the VSP electronically can be found at <http://www.uscg.mil/HQ/MSC>.

(c) The VSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the VSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.

§ 104.405 Format of the Vessel Security Plan (VSP).

(a) A vessel owner or operator must ensure that the VSP consists of the individual sections listed in this paragraph. If the VSP does not follow the order as it appears in the list, the vessel owner or operator must ensure that the VSP contains an index identifying the location of each of the following sections:

- (1) Security organization of the vessel;
- (2) Personnel training;

- (3) Drills and exercises;
- (4) Records and documentation;
- (5) Response to change in MARSEC Level;
- (6) Procedures for interfacing with facilities and other vessels;
- (7) Declarations of Security (DoS);
- (8) Communications;
- (9) Security systems and equipment maintenance;
- (10) Security measures for access control;
- (11) Security measures for restricted areas;
- (12) Security measures for handling cargo;
- (13) Security measures for delivery of vessel stores and bunkers;
- (14) Security measures for monitoring;
- (15) Security incident procedures;
- (16) Audits and Vessel Security Plan (VSP) amendments; and
- (17) Vessel Security Assessment (VSA) Report.

(b) The VSP must describe in detail how the requirements of subpart B of this part will be met.

§ 104.410 Submission and approval.

(a) On or before [Insert date 180 days after publication in the Federal Register], each vessel owner or operator must either:

(1) Submit one copy of their Vessel Security Plan (VSP) for review and approval to the Commanding Officer, Marine Safety Center (MSC) and a letter certifying that the VSP meets applicable requirements of this part; or

(2) If implementing a Coast Guard approved Alternative Security Program, meet the requirements in § 101.120(b) of this subchapter.

(b) Vessels built on or after July 1, 2004, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations.

(c) The Commanding Officer, Marine Safety Center (MSC), 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, or

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

(d) A VSP may be submitted and approved to cover more than one vessel where the vessel design and operations are similar.

(e) Each company or vessel, owner or operator, that submits one VSP to cover two or more vessels of similar design and operation must address vessel-specific

information that includes the physical and operational characteristics of each vessel.

(f) A plan that is approved by the MSC is valid for five years from the date of its approval.

§ 104.415 Amendment and audit.

(a) Amendments.--

(1) Amendments to a Vessel Security Plan that are approved by the MSC may be initiated by:

(i) The vessel owner or operator; or

(ii) The Coast Guard upon a determination that an amendment is needed to maintain the vessel's security. The Coast Guard will give the vessel owner or operator written notice and request that the vessel owner or operator propose amendments addressing any matters specified in the notice. The company owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the company owner or operator shall ensure temporary security measures are implemented to the satisfaction of the Coast Guard.

(2) Proposed amendments must be sent to the marine safety center at the address shown in § 104.400(b) of this part. If initiated by the company or vessel, owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the

Marine Safety Center (MSC) allows a shorter period. The MSC will approve or disapprove the proposed amendment in accordance with § 104.410 of this part.

(3) If the owner or operator has changed, the Vessel Security Officer (VSO) must amend the Vessel Security Plan (VSP) to include the name and contact information of the new vessel owner or operator and submit the affected portion of the VSP for review and approval in accordance with § 104.410 of this part.

(b) Audits.--

(1) The CSO or VSO must ensure an audit of the VSP is performed annually, beginning no later than one year from the initial date of approval and attach a letter to the VSP certifying that the VSP meets the applicable requirements of this part.

(2) The VSP must be audited if there is a change in the company's or vessel's ownership or operator, or if there have been modifications to the vessel, including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) Auditing the VSP as a result of modifications to the vessel may be limited to those sections of the VSP affected by the vessel modifications.

(4) Unless impracticable due to the size and nature of the company or the vessel, personnel conducting internal audits of the security measures specified in the VSP or evaluating its implementation must:

- (i) Have knowledge of methods of conducting audits and inspections, and control and monitoring techniques;
- (ii) Not have regularly assigned security duties; and
- (iii) Be independent of any security measures being audited.

(5) If the results of an audit require amendment of either the VSA or VSP, the VSO or CSO must submit, in accordance with § 104.410 of this part, the amendments to the MSC for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended VSP meets the applicable requirements of this part.

PART 160--PORTS AND WATERWAY SAFETY--GENERAL

2. Revise the authority citation for part 160 to read as follows:

Authority: 33 U.S.C. 1223, 1231; 46 U.S.C. Chapter 701; Department of Homeland Security Delegation 0170. Subpart D is also issued under the authority of 33 U.S.C. 125 and 46 U.S.C. 3715.

3. In § 160.203, add paragraph (f) to read as follows:

§ 160.203 Exemptions.

(f) U.S. vessels need not submit the International Ship and Port Facility Code (ISPS) Notice information (Entry (9) to Table 160.206).

4. In § 160.206, in the table in paragraph (a), add paragraph (9) to read as follows:

§ 160.206 Information required in an NOA.

* * * * *

Table 160.206. NOA Information Items.

Required information	Vessels not carrying CDC	Vessels carrying CDC	
		Vessels	Towing vessels controlling vessels carrying CDC
* * * * *			
(9) International Ship and Port Facility Code (ISPS) Notice*:			
(i) The date of issuance for the vessel's International Ship Security Certificate (ISSC), if any;	X	X	X
(ii) Whether the ISSC, if any, is an initial Interim ISSC, subsequent and consecutive Interim ISSC, or final ISSC;	X	X	X
(iii) Declaration that the approved ship security plan, if any, is being implemented;	X	X	X
(iv) If a subsequent and consecutive Interim ISSC, the reasons therefor;	X	X	X
(v) The name and 24-hour contact information for the Company Security Officer; and	X	X	X
(vi) The name of the Flag Administration, or the recognized security organization(s) representing the vessel flag Administration that issued the ISSC.	X	X	X

*The information required by items 9(i)-(iii) need not be submitted before January 1, 2004. All other information required by item 9 need not be submitted before July 1, 2004.

* * * * *

33 CFR PART 165--REGULATED NAVIGATION AREAS AND LIMITED
ACCESS AREAS

5. Revise the authority citation for part 165 to read
as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter
701; 50 U.S.C. 191, 195; 33 CFR 1.05-1(g), 6.04-1, 6.04-6
and 160.5; Pub.L. 107-295, 116 Stat. 2064; Department of
Homeland Security Delegation 0170.

* * * * *

46 PART 2--VESSEL INSPECTIONS

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

Authority: 33 U.S.C. 1903; 43 U.S.C. 1333; 46 U.S.C.
3103, 3205, 3306, 3307, 3703; 46 U.S.C. Chapter 701;
Executive Order 12234, 45 FR 58801, 3 CFR, 1980 Comp., p.
277; Department of Homeland Security Delegation 0170;
subpart 2.45 also issued under the authority of Act Dec.
27, 1950, Ch. 1155, secs. 1, 2, 64 Stat. 1120 (see 46
U.S.C. App. Note prec. 1).

7. In § 2.01-25, add new paragraph (a)(1)(viii) to
read as follows:

§ 2.01-25 International Convention for Safety of Life at
Sea (SOLAS), 1974.

(a) * * *

(1) * * *

(viii) International Ship Security Certificate.

* * * * *

PART 31--INSPECTION AND CERTIFICATION

8. Revise the authority citation for part 31 to read as follows:

Authority: 33 U.S.C. 1321(j); 43 U.S.C. 2103, 3205, 3306, 3307, 3703; 46 U.S.C. Chapter 701; 49 U.S.C. 5103, 5106; Executive Order 12234, 45 FR 58801, 3 CFR, 1980 Comp., p. 277; Executive Order 12777, 56 FR 54757, 3 CFR, 1991 Comp., p. 351; Department of Homeland Security Delegation 0170; Section 31.10-021 also issued under the authority § 4109, Public Law 101-380, 104 Stat. 515.

9. Revise § 31.05-1(a) to read as follows:

§ 31.05-1 Issuance of certificate of inspection -- TB/ALL.

(a) When a tank vessel is found to comply with all applicable regulations, including the applicable provisions of subchapters E, F, J, O, Q, S, and W of this chapter and of 33 CFR parts 104, 155, and 157, the Officer in Charge, Marine Inspection will issue a certificate of inspection to the vessel or to its owners.

* * * * *

PART 71--INSPECTION AND CERTIFICATION

10. Revise the authority citation for part 71 to read as follows:

Authority: 33 U.S.C. 1321(j); 46 U.S.C. 2113, 3205, 3306, 3307; 46 U.S.C. Chapter 701; Executive Order 12234, 45 FR 58801, 3 CFR, 1980 Comp., p. 277; Executive Order 12777, 56 FR 54757, 3 CFR, 1991 Comp., p. 351; Department of Homeland Security Delegation 0170.

11. Add new § 71.25-47 to read as follows:

§ 91.25-47 Vessel security.

At each inspection for certification and periodic inspection, the inspector shall examine the vessel to determine that it meets vessel security requirements in 33 CFR part 104.

PART 91--INSPECTION AND CERTIFICATION

12. Revise the authority citation for part 91 to read as follows:

Authority: 33 U.S.C. 1321(j); 46 U.S.C. 3205, 3306, 3307; 46 U.S.C. Chapter 701; Executive Order 12234; 45 FR 58801; 3 CFR, 1980 Comp., p. 277; Executive Order 12777, 56 FR 54757, 3 CFR, 1991 Comp., p. 351; Department of Homeland Security Delegation 0170.

13. Add new § 91.25-47 to read as follows:

§ 91.25-47 Vessel security.

At each inspection for certification and periodic inspection, the inspector shall examine the vessel to determine that it meets vessel security requirements in 33 CFR part 104.

PART 115--INSPECTION AND CERTIFICATION

14. Revise the authority citation for part 115 to read as follows:

Authority: 33 U.S.C. 1321(j); 46 U.S.C. 2103, 3205, 3306, 3307; 46 U.S.C. Chapter 701; 49 U.S.C. App. 1804; Executive Order 11735, 38 FR 21243, 3 CFR, 1971-1975 Comp., p. 743; Executive Order 12234, 45 FR 58801, 3 CFR, 1980 Comp., p. 277; Department of Homeland Security Delegation 0170.

15. Revise § 115.404(a) to read as follows:

§ 115.404 Subsequent inspections for certification.

(a) An inspection for renewal of a Certificate of Inspection is conducted to determine if the vessel is in satisfactory condition, fit for the service intended, and complies with all applicable regulations. It normally includes inspection and testing of the structure, machinery, equipment, and on a sailing vessel, rigging and sails. The owner or operator must conduct all tests as required by the OCMI, and make the vessel available for all specific inspections and drills required by subpart H of this part. In addition, the OCMI may require the vessel to get underway.

* * * * *

PART 126--INSPECTION AND CERTIFICATION

16. Revise the authority citation for part 126 to read as follows:

Authority: 33 U.S.C. 1321(j); 46 U.S.C. 3205, 3306, 3307; 46 U.S.C. Chapter 701; Executive Order 111735, 38 FR 21243, 3 CFR 1971-1975 Comp., p. 793; Department of Homeland Security Delegation 0170.

17. Add new § 126.490 to read as follows:

§ 126.490 Vessel security.

At each inspection for certification and periodic inspection, the inspector shall examine the vessel to

determine that it meets vessel security requirements in 33 CFR part 104.

PART 176--INSPECTION AND CERTIFICATION

18. Revise the authority citation for part 176 to read as follows:

Authority: 33 U.S.C. 1321(j); 46 U.S.C. 2103, 3205, 3306, 3307; 46 U.S.C. Chapter 701; 49 U.S.C. App. 1804; Executive Order 11735, 38 FR 21243, 3 CFR, 1971-1975 Comp., p. 277; Department of Homeland Security Delegation 0170.

19. Revise § 176.404(a) to read as follows:

§ 176.404 Subsequent inspections for certification.

(a) An inspection for renewal of a Certificate of Inspection is conducted to determine if the vessel is in satisfactory condition, fit for the service intended, and complies with all applicable regulations. It normally includes inspection and testing of the structure, machinery, equipment, and on a sailing vessel, rigging and sails. The owner or operator must conduct all tests as required by the OCMI, and make the vessel available for all specific inspections and drills required by subpart H of this part. In addition, the OCMI may require the vessel to get underway.

* * * * *

Dated: June 23, 2003.

THOMAS H. COLLINS
Admiral, U.S. Coast Guard
Commandant