

DEPARTMENT OF HOMELAND SECURITY

COAST GUARD

33 CFR Part 105

[USCG-2003-14732]

RIN 1625-AA43

Facility 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 facilities in U.S. ports. It requires owners or operators of facilities to designate security officers for facilities, develop security plans based on security assessments and surveys, implement security measures specific to the facilities' operations, 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 Safety of Life at Sea, 1974. To best understand these interim rules, first read the one titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792, published elsewhere in today's Federal Register).

DATES:

Effective date. This interim rule is effective from [Insert date of publication in the FEDERAL REGISTER.] until November 25, 2003.

Comments. Comments and related material must reach the Docket Management Facility on or before [Insert date 30 days after date of publication in the FEDERAL REGISTER.].

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-2003-14732), 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 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.

FOR FURTHER INFORMATION CONTACT: If you have questions on this interim rule, call Lieutenant Gregory Purvis, 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, at 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 of 2002 (MTSA, Public Law 107-295, 116 STAT. 2064), 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>.

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/>.

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-2003-14732), 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 indicate 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 interim rule in view of them.

Public Meeting

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 interim rule effective upon publication. Section 102(d)(1) of the MTSA 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 Facility Issues in the
Notice of Meeting

For a discussion of comments on facilities 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

The purpose of this rulemaking is to require security measures for facilities in order to reduce the risk of and to mitigate the results of an act that threatens the security of personnel, the facility, and the public. This rulemaking combines international requirements and existing domestic policy, and adds part 105, Facility 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) published elsewhere in today's Federal Register.

This rulemaking applies to facilities subject to 33 CFR parts 126, 127, and 154; facilities that receive vessels certified to carry more than 150 passengers; and

facilities that receive vessels on international voyages, including vessels solely navigating the Great Lakes.

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.

This rulemaking does not apply to Outer Continental Shelf (OCS) platforms and deepwater ports. Those structures are covered by the rulemaking "Outer Continental Shelf Facility Security" (USCG-2003-14759), published elsewhere in today's Federal Register.

This preamble describes the facilities regulated by part 105 and the requirements for conducting Facility Security Assessments, developing Facility Security Plans, and implementing security measures and procedures. The requirements in part 105 are consistent with requirements in the ISPS Code. Facility security includes the requirements discussed below:

Compliance.

The Coast Guard, as provided in 33 CFR part 126, 127, and 154, will verify facility compliance with this part during inspections.

As required by Regulation 3 of Chapter XI-2 of the International Convention for Safety of Life at Sea, 1974 (SOLAS) and the ISPS Code, part A, section 5, the Coast Guard has published additional requirements that provide the U.S. (as a contracting government) with requirements for setting and communicating changes in Maritime Security (MARSEC) Level, completing Declarations of Security, and additional instructions for all facilities when MARSEC Level 3 is set.

Waivers.

The waiver section details procedures for requesting a waiver for the benefit of facility 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 facility 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 facilities 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 who choose to implement an appropriate Alternative Security Program will be required to implement it in its entirety to be deemed in compliance with this part.

Evaluating submissions of Waivers, Equivalentents, 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.

Facility Owner or Operator Responsibilities.

This rule requires each facility owner or operator to develop an effective security plan that incorporates detailed preparation, prevention, and response activities for each MARSEC Level, and detail the organizations, or personnel responsible for carrying out those activities. The requirements discussed in this subpart are also consistent with requirements in the ISPS Code. Facility owner or operator responsibilities include:

- Designating a Facility Security Officer.
- Ensuring a Facility Security Assessment is conducted.
- Developing and submitting for approval a Facility Security Plan.
- Operating the facility in accordance with the approved Facility Security Plan.
- Implementing additional security measures required by changes in MARSEC Level.
- Reporting all breaches of security and security incidents.
- Coordinating 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, in advance

of a vessel's arrival. (In the past, some facilities may have denied access to seafarers and seafarer welfare organizations where there was not an articulable security basis for doing so. The Coast Guard is including their provision in this interim rule to encourage facilities to allow such access when appropriate.)

Facility Security Officer (FSO).

This rule requires that a facility owner or operator designate in writing a Facility Security Officer for each facility. The Facility Security Officer may be a full-time or collateral-duty position. The Facility Security Officer must have general knowledge on a range of issues such as security administration, relevant international laws, domestic regulations, current security threats and patterns, risk assessment methodology, inspections, control procedures and conducting audits. The most important duties that must be performed by the Facility Security Officer would include implementing a Facility Security Plan; periodically auditing and updating the Facility Security Assessment and Facility Security Plan; ensuring that adequate training is provided to facility personnel; and ensuring the facility is operating in accordance with the plan and in continuous compliance with part 105. The

Facility Security Officer may assign security duties to other facility personnel; however, the Facility Security Officer remains responsible for these duties.

Training.

Required training for facility personnel must be specified in the Facility Security Plan. Specific security training courses for the Facility Security Officer and facility personnel will not be required by the Coast Guard. While formal training may be appropriate, we are not mandating specifics. Facility 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 Facility Security Officer is also required to ensure that facility security persons possess necessary training to maintain the overall security of the facility.

Drill and Exercise 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 no 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 facility 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 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 facility owner or operator must develop security incident procedures for responding to transportation security incidents. The security incident procedures must explain the facility'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 facility and evacuating personnel, as well as actions for securing vessels moored to the facility and evacuating passengers and crew.

Declaration of Security (DoS).

A Declaration of Security is a written agreement between the facility and a vessel that 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 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, in bulk, will complete a Declaration of Security for every evolution regardless of the MARSEC Level. At MARSEC Levels 2 and 3, all vessels and facilities would need to complete the Declaration of Security.

Facilities that frequently receive the same vessel 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-facility interfaces. Declarations of Security must be kept as part of the facility's recordkeeping.

Facility Security Assessment (FSA).

This rule requires all regulated facilities to complete a Facility Security Assessment, which is an essential and integral part of the process of developing and updating the required Facility Security Plan. The Facility Security Plan is based on the results of the Facility Security Assessment. The Facility Security Officer must examine and evaluate existing facility protective measures, procedures, and operations.

The Facility Security Officer must also examine each identified point of access, including rail access, roads, waterside, and gates, and evaluate its potential for use by individuals who might engage in unlawful acts, including individuals with legitimate access, as well as those seeking unauthorized entry.

Each facility owner or operator is required to document and retain its Facility Security Assessment for a period of 5 years. Prior to conducting a Facility Security Assessment, the Facility Security Officer is responsible for researching and using available information on the assessment of threat for the port at which the facility is located, as well as vessels that would call on the facility. The first step in the facility security process is to conduct an on-scene survey. The on-scene survey is used to examine and evaluate existing facility protective measures, procedures and operations. In conducting the Facility Security Assessment, the facility owner or operator must ensure that the Facility Security Officer analyzes the facility background information and the results of the on scene survey, and considering the requirements of this interim rule, provide recommendation to establish and prioritize the security measures that should be included in the Facility Security Plan. The

facility owner or operator then must ensure that a written Facility Security Assessment report is prepared and included in the Facility Security Plan. The Facility Security Assessment must be reviewed and updated each time the Facility Security Plan is revised and when the Facility Security Plan is submitted for re-approval every five years. The facility owner or operator then must ensure that a written Facility Security Assessment report is prepared and included as an appendix to the Facility Security Plan.

The Facility Security Officer is also responsible for ensuring that the Facility Security Assessment is periodically reviewed and updated, taking into account changes in the facility and its operations. Before a plan could be renewed or revised, a new Facility Security Assessment would need to be conducted.

The Facility Security Officer is responsible for obtaining and recording any specific information required to conduct the Facility Security Assessment.

Facility Security Plan (FSP).

This subpart contains requirements for Facility Security Plans. The requirements discussed in this subpart are consistent with requirements in the ISPS Code.

Facility Security Plans must incorporate the results of the required Facility Security Assessment and consider the recommended measures appropriate to each facility.

Facility Security Plans can be combined with or complement existing safety management systems. The plans may be kept in an electronic format, protected by means to prevent it from being deleted, destroyed or overwritten. The plans must also be protected from unauthorized access or disclosure.

Facility Security Plans required under this rulemaking must contain:

- A list of measures and equipment needed to prevent or deter dangerous substances and devices which could be used against people, vessels or ports and the carriage of which is not authorized from being introduced by any means on to the facility;
- Requirements for the prevention of unauthorized access to the facility and to restricted areas of the facility;
- Documented procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the facility or the vessel-to-port interface;

- Documented procedures for evacuation in case of security threats or breaches of security;
- Procedures for training, exercises, and drills associated with the plan;
- Documented procedures for interfacing with port and vessel security activities;
- Documented procedures for the periodic review of the Facility Security Plan and for updating it;
- Documented procedures for reporting security incidents;
- Written designation of the Facility Security Officer;
- A list of the duties and responsibilities of all facility personnel with a security role;
- A list of measures to ensure the security of information contained in the plan;
- A maintenance system to maintain operational readiness of all required equipment using manufacturers' recommended maintenance instructions and periodic inspection;
- A list of measures needed to ensure effective security of cargo, cargo processing, and the cargo-handling equipment at the facility; and

- A completed Facility Vulnerability and Security Measures Summary (Form CG-6025) for each facility covered by the Plan.

Submission and Approval of Security Plan.

The Facility Security Plan, including the Facility Security Assessment report and the Facility Vulnerability and Security Measures Summary (Form CG-6025), must be submitted to and reviewed by the cognizant COTP. Once the COTP finds that the plan meets the security requirements in part 105, the submitter will receive an approval letter that may contain conditions of the approval.

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

If the COTP finds that the Facility Security Plan does not meet the security requirements, the plans would be returned to the facility with a disapproval letter with an explanation of why the plan does not meet the part 105 requirements.

Security plans must be reviewed by the Coast Guard every time:

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

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. A summary of the Assessment follows:

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 will not implement this interim rule exactly as presented in the assessment. Depending on each company's choices, some companies could spend much less than what is estimated herein while others could spend significantly more. In general, we assume that each company will implement this interim rule differently based on the type of facilities it owns or operates and whether it engages in international or domestic trade.

The population affected by this interim rule is approximately 5,000 facilities, and the estimated Present Value (PV) cost to these facilities is approximately PV \$5.399 billion (2003 to 2012, 7 percent discount rate). Approximately PV \$2.718 billion of this total is attributed to facilities engaged in the transfer of hazardous bulk liquids (petroleum, edible oils, and liquefied gases). The remaining PV \$2.681 billion is attributable to facilities that receive vessels on international voyages or carry more than 150 passengers, or fleet barges carrying certain dangerous cargoes. During the initial year of compliance, the cost is attributable to purchasing and installing

equipment, hiring security officers, and preparing paperwork. The initial cost is an estimated \$1.125 billion (non-discounted, \$498 million for the facilities with hazardous bulk liquids, \$627 million for the other facilities). Following initial implementation, the annual cost is an estimated \$656 million (non-discounted, \$341 million for the facilities with hazardous bulk liquids, \$315 million for the other facilities).

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

Benefit Assessment

This rule is one of six interim rules that implement national maritime security initiatives concerning general provisions, Area Maritime Security (ports), vessels, facilities, Outer Continental Shelf 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, Outer Continental Shelf 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" (USGC-2003-14792) published elsewhere in today's Federal Register. For this benefit assessment, the Coast Guard used a team of experts 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 indicates 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 must ensure, 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 Facility Security Plans for the affected population reduces 473,659 risk points annually through 2012. The benefits attributable for part 101-General Provisions—were not considered separately since it is an overarching section for all the parts.

Table 1. Annual Risk Points Reduced by the 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 (seven 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 have 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.

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

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

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

them may need to install or upgrade fences or lighting equipment.

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

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

Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (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 rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please consult LT Gregory Purvis 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 an existing OMB-approved collection – 1625-0077 [formerly 2115-0557]. A summary of the revised collection follows.

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 facilities to draft and maintain Facility Security Assessments and Facility Security Plans. It also requires that, under certain circumstances, documentation and letters be provided to the Coast Guard to ensure compliance with the security requirements. Finally, the Coast Guard requires that a Declaration of Security be

completed between facilities and vessels handling certain types of cargo.

NEED FOR INFORMATION: The primary need for information is to identify the adequate security mitigating measures that will be implemented when needed. Additionally, the Coast Guard intends to collect a summary of the vulnerabilities and selected security measures from the facilities regulated under this rule. The data will be submitted on form CG-6025, Facility Vulnerability and Security Measures Summary. Electronic submission when available will be accepted and encouraged. The form must be included in the Facility Security Plan as an annex to assist COTPs in the development of the Area Maritime Security Plan.

PROPOSED USE OF INFORMATION: The information will be used to identify and communicate the security mitigating measures to the Coast Guard and necessary personnel. Declarations of Security will be used by some facilities and vessels to identify and delineate the security responsibilities between a vessel and a facility.

DESCRIPTION OF THE RESPONDENTS: The Facility Security Officer or another designated person is responsible for developing the Facility Security Assessment and the Facility Security Plan. For some facilities, the Facility

Security Officer will also complete a Declaration of Security.

NUMBER OF RESPONDENTS: 4,965 Facility Security Officers.

FREQUENCY OF RESPONSE: Facility Security Assessments and Facility Security Plans are to be submitted for approval initially, and will be reviewed annually. Declarations of Security are to be completed whenever certain vessels are being serviced by a facility.

BURDEN OF RESPONSE: The burden of developing each Facility Security Assessment and each Facility Security Plan is estimated to take 80 hours for some facilities and 40 hours for others. Updating each assessment or plan is estimated to take 4 hours for some facilities and 2 hours for others. Each Declaration of Security is expected to be 15 minutes.

ESTIMATE OF TOTAL ANNUAL BURDEN: Facility Security Assessments and Facility Security Plans will have a total burden in the initial year of 528,240 hours (264,120 for the assessments and 264,120 for the plans). Annually, the total burden of the assessments and the plans is 26,412 hours (13,206 for the assessments and 13,206 for the plans). Declarations of Security will have an annual burden of 581,775 hours. The total burden hours for this

interim rule are 528,240 hours in the initial year, and 608,187 hours in subsequent years. 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.

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 the collection of information on June 16, 2003. It is 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 the collection of information on June 16, 2003. It is valid until December 31, 2003.

Federalism

A rule has implications for federalism under Executive Order 13132, Federalism, if it has a substantial direct effect on State or local governments and would either preempt State law or impose a substantial direct cost of compliance on them. 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 detailed of the 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 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.

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 rule and concluded that under figure 2-1, paragraph (34) (a) and (34) (c), of Commandant Instruction M16475.1D, this 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 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 rule will be done in conjunction with appropriate State coastal authorities. The Coast Guard will, therefore, comply with the requirements of the Coastal Zone Management Act while furthering its intent to protect the coastal zone.

List of Subjects in 33 CFR Part 105

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

Dated: June 23, 2003

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

For the reasons discussed in the preamble, the Coast Guard adds part 105 to subchapter H of chapter I of title 33 in the CFR to read as follows:

Part 105—Facility Security

Subpart A—General

105.100 Definitions.

105.105 Applicability.

- 105.106 Public access areas.
- 105.110 Exemptions.
- 105.115 Compliance dates.
- 105.120 Compliance documentation.
- 105.125 Noncompliance.
- 105.130 Waivers.
- 105.135 Equivalents.
- 105.140 Alternative Security Program.
- 105.145 Maritime Security (MARSEC) Directive.
- 105.150 Right to appeal.

Subpart B—Facility Security Requirements

- 105.200 Owner or operator.
- 105.205 Facility Security Officer (FSO).
- 105.210 Facility personnel with security duties.
- 105.215 Security training for all other facility personnel.
- 105.220 Drill and exercise requirements.
- 105.225 Facility recordkeeping requirements.
- 105.230 Maritime Security (MARSEC) Level coordination and implementation.
- 105.235 Communications.
- 105.240 Procedures for interfacing with vessels.
- 105.245 Declaration of Security (DoS).

- 105.250 Security systems and equipment maintenance.
 - 105.255 Security measures for access control.
 - 105.260 Security measures for restricted areas.
 - 105.265 Security measures for handling cargo.
 - 105.270 Security measures for delivery of vessel stores and bunkers.
 - 105.275 Security measures for monitoring.
 - 105.280 Security incident procedures.
 - 105.285 Additional requirements—passenger and ferry facilities.
 - 105.290 Additional requirements—cruise ship terminals.
 - 105.295 Additional requirements—Certain Dangerous Cargo (CDC) facilities.
 - 105.296 Additional requirements—barge fleeting facilities.
- Subpart C—Facility Security Assessment (FSA)
- 105.300 General.
 - 105.305 Facility Security Assessment (FSA) requirements.
 - 105.310 Submission requirements.
- Subpart D—Facility Security Plan (FSP)
- 105.400 General.
 - 105.405 Format and content of the Facility Security Plan (FSP).

105.410 Submission and approval.

105.415 Amendment and audit.

Appendix A to part 105—Facility Vulnerability and Security Measure Summary (CG-6025).

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70103; 50 U.S.C. 191; 33 C.F.R. 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.

Subpart A—General

§ 105.100 Definitions.

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

§ 105.105 Applicability.

(a) The requirements in this part apply to the owner or operator of any U.S.:

(1) Facility subject to 33 CFR parts 126, 127, or 154;

(2) Facility that receives vessels certificated to carry more than 150 passengers;

(3) Facility that receives vessels subject to the International Convention for Safety of Life at Sea, 1974, or that are commercial vessels subject to subchapter I of Title 46, Code of Federal Regulations, greater than 100 gross register tons on international voyages, including vessels solely navigating the Great Lakes; or

(4) Fleeting facility that receives barges carrying, in bulk, cargoes regulated by subchapters D and O of chapter I, title 46, Code of Federal Regulations or Certain Dangerous Cargoes.

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

(c) This part does not apply to the owner or operator of the following U.S. facilities:

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

(2) An oil and natural gas production, exploration, or development facility regulated by 33 CFR parts 126 or 154 if:

(i) The facility is engaged solely in the exploration, development, or production of oil and natural gas; and

(ii) The facility does not meet or exceed the operating conditions in § 106.105 of this subchapter;

(3) A facility that supports the production, exploration, or development of oil and natural gas regulated by 33 CFR parts 126 or 154 if:

(i) The facility is engaged solely in the support of exploration, development, or production of oil and natural gas; and

(ii) The facility transports or stores quantities of hazardous materials that do not meet and exceed those specified in 49 CFR 172.800(b)(1)-(6); or

(iii) The facility stores less than 42,000 gallons of cargo regulated by 33 CFR part 154;

(4) A mobile facility regulated by 33 CFR 154; or

(5) An isolated facility that receives materials regulated by 33 CFR parts 126 or 154 by vessel due to the lack of road access to the facility and does not distribute the material through secondary marine transfers.

§ 105.106 Public access areas.

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

(b) A public access area is a defined space within a facility that is open to all persons and provides access through the facility from public thoroughfares to the vessel.

§ 105.110 Exemptions.

(a) An owner or operator of any barge fleeting facility subject to this part is exempt from complying with § 105.265, Security measures for handling cargo; and § 105.270, Security measures for delivery of vessel stores and bunkers.

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

§ 105.115 Compliance dates.

(a) On or before [Insert date 180 days after publication in the Federal Register], each facility owner or operator must submit to the cognizant COTP for each facility a Facility Security Plan (FSP) described in subpart D of this part for review and approval.

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

§ 105.120 Compliance documentation.

Each facility owner or operator subject to this part must ensure, no later than July 1, 2004, that copies of the following documentation are available at the facility and are made available to the Coast Guard upon request:

(a) The approved Facility Security Plan (FSP), as well as any approved revisions or amendments thereto, and a letter of approval from the COTP dated within the last 5 years;

(b) The FSP submitted for approval and an acknowledgement letter from the COTP stating that the Coast Guard is currently reviewing the FSP submitted for approval, and that the facility may continue to operate so long as the facility remains in compliance with the submitted FSP; or

(c) For facilities operating under a Coast Guard-approved Alternative Security Program as provided in § 105.140, a copy of the Alternative Security Program the facility is using and a letter signed by the facility owner or operator, stating which Alternative Security Program the facility is using and certifying that the facility is in full compliance with that program.

§ 105.125 Noncompliance.

When a facility is not in compliance with the requirements of this part, the facility owner or operator must notify the cognizant COTP and request a waiver to continue operations.

§ 105.130 Waivers.

Any facility owner or operator may apply for a waiver of any requirement of this part that the facility owner or operator considers unnecessary in light of the nature or operating conditions of the facility, prior to operating. 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 facility owner or operator to provide data for use in 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 facility, its employees, visiting vessels, or ports. The Commandant (G-MP) may grant a waiver with or without written conditions only if the waiver will not reduce the overall security of the facility, its employees, visiting vessels, or port.

§ 105.135 Equivalents.

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

§ 105.140 Alternative Security Program.

(a) A facility owner or operator may use an Alternative Security Program approved under § 101.120 of this subchapter if:

(1) The Alternative Security Program is appropriate to that facility;

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

(b) A facility owner or operator using an Alternative Security Program approved under § 101.120 of this subchapter must complete and submit to the cognizant COTP a Facility Vulnerability and Security Measures Summary (Form CG-6025) in appendix A to part 105—Facility Vulnerability and Security (CG-6025).

§ 105.145 Maritime Security (MARSEC) Directive.

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

§ 105.150 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—Facility Security Requirements

§ 105.200 Owner or operator.

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

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

(1) Define the security organizational structure and provide each person exercising security duties and responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate, in writing, by name or by title, a Facility Security Officer (FSO) and identify how the officer can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of a Facility Security Plan (FSP);

(5) Ensure that the facility operates in compliance with the approved FSP;

(6) Ensure that adequate coordination of security issues takes place between the facility and vessels that call on it, including the execution of a Declaration of Security (DoS) as required by this part;

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

(8) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level; and

(9) Ensure the report of all breaches of security and security incidents to the National Response Center in accordance with part 101 of this subchapter.

§ 105.205 Facility Security Officer (FSO).

(a) General.--

(1) The FSO 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 FSO.

(2) The same person may serve as the FSO for more than one facility, provided the facilities are in the same COTP zone and are not more than 50 miles apart. If a person serves as the FSO for more than one facility, the name of each facility for which he or she is the FSO must

be listed in the Facility Security Plan (FSP) of each facility for which or she is the FSO.

(3) The FSO may assign security duties to other facility personnel; however, the FSO retains the responsibility for these duties.

(b) Qualifications.--

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

(i) Security organization of the facility;

(ii) General vessel and facility operations and conditions;

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

(iv) Emergency preparedness, response, and contingency planning;

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

(vi) Methods of conducting audits, inspections, control, and monitoring techniques.

(2) In addition to knowledge and training required in paragraph (b)(1) of this section, the FSO must have knowledge of and receive training in the following, as appropriate:

- (i) Relevant international laws and codes, and recommendations;
- (ii) Relevant government legislation and regulations;
- (iii) Responsibilities and functions of local, State, and Federal law enforcement agencies;
- (iv) Risk assessment methodology;
- (v) Methods of facility 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) Current security threats and patterns;
- (ix) Recognizing and detecting dangerous substances and devices;
- (x) Recognizing characteristics and behavioral patterns of persons who are likely to threaten security;
- (xi) Techniques used to circumvent security measures;
- (xii) Conducting physical searches and non-intrusive inspections;
- (xiii) Conducting security drills and exercises, including exercises with vessels; and
- (xiv) Assessing security drills and exercises.

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

(1) Ensure that the Facility Security Assessment (FSA) is conducted;

(2) Ensure the development and implementation of a FSP;

(3) Ensure that an annual audit is conducted, and if necessary if the FSA and FSP are updated;

(4) Ensure the FSP is exercised per § 105.220 of this part;

(5) Ensure that regular security inspections of the facility are conducted;

(6) Ensure the security awareness and vigilance of the facility personnel;

(7) Ensure adequate training to personnel performing facility security duties;

(8) Ensure that occurrences that threaten the security of the facility are recorded and reported to the owner or operator;

(9) Ensure the maintenance of records required by this part;

(10) Ensure the preparation and the submission of any reports as required by this part;

(11) Ensure the execution of any required Declarations of Security with Vessel Security Officers;

(12) Ensure the coordination of security services in accordance with the approved FSP;

(13) Ensure that security equipment is properly operated, tested, calibrated, and maintained;

(14) Ensure the recording and reporting of attainment changes in MARSEC Levels to the owner or operator and the cognizant COTP;

(15) When requested, ensure that the Vessel Security Officers receive assistance in confirming the identity of visitors and service providers seeking to board the vessel through the facility;

(16) Ensure notification, as soon as possible, to law enforcement personnel and other emergency responders to permit a timely response to any transportation security incident;

(17) Ensure that the FSP is submitted to the cognizant COTP for approval, as well as any plans to change the facility or facility infrastructure prior to amending the FSP; and

(18) Ensure that all facility personnel are briefed of changes in security conditions at the facility.

§ 105.210 Facility personnel with security duties.

Facility 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, calibration, and maintenance of security equipment and systems;
- (j) Inspection, control, and monitoring techniques;
- (k) Relevant provisions of the Facility Security Plan (FSP);

(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 MARSEC Levels.

§ 105.215 Security training for all other facility personnel.

All other facility 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 Facility Security Plan (FSP);

(b) The meaning and the consequential requirements of the different MARSEC Levels as they apply to them, 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.

§ 105.220 Drill and exercise requirements.

(a) General. Drills and exercises must test the proficiency of facility personnel in assigned security

duties at all MARSEC Levels and the effective implementation of the Facility Security Plan (FSP). They must enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

(b) Drills.--

(1) The FSO must ensure that at least one security drill is conducted every three months. Security drills may be held in conjunction with non-security drills, where appropriate.

(2) Drills must test individual elements of the FSP, including response to security threats and incidents. Drills should take into account the types of operations of the facility, facility personnel changes, the type of vessel the facility is serving, 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 a vessel is moored at the facility on the date the facility has planned to conduct any drills, the facility cannot require the vessel or vessel personnel to be a part of or participate in the facility's scheduled drill.

(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 facility-specific or part of a cooperative exercise program with 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 substantial and active participation of FSOs, and may include government authorities and vessels visiting the facility. Requests for participation of Company and Vessel Security Officers in joint exercises should consider the security and work implications for the vessel.

§ 105.225 Facility recordkeeping requirements.

(a) Unless otherwise specified in this section, the Facility Security Officer (FSO) 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 Facility Security Plan (FSP);

(3) Incidents and Breaches of security. For each incident or breach of security, the date and time of occurrence, location within the facility, description of incident or breaches, to whom it was reported, and description of the response;

(4) Changes in MARSEC Levels. For each change in MARSEC Level, the 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, record the date and time, and the specific security equipment involved;

(6) Security threats. For each security threat, the 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) A copy of each single-visit DoS 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 FSP. For each annual audit, a letter certified by the FSO stating the date the audit was completed.

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

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

(a) The facility owner or operator must ensure the facility operates in compliance with the security

requirements in this part for the MARSEC Level in effect for the port.

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

(1) Vessels moored to the facility and vessels scheduled to arrive at the facility within 96 hours of the MARSEC Level change are notified of the new MARSEC Level and the Declaration of Security is revised as necessary;

(2) The facility complies with the required additional security measures within 12 hours; and

(3) The facility reports compliance or noncompliance to the COTP.

(c) For MARSEC Levels 2 and 3, the Facility Security Officer must inform all facility personnel about identified threats, and emphasize reporting procedures and stress the need for increased vigilance.

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

(e) At MARSEC Level 3, in addition to the requirements in this part, a facility 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) Use of waterborne security patrol;
- (2) Use of armed security personnel to control access to the facility and to deter, to the maximum extent practical, a transportation security incident; and
- (3) Examination of piers, wharves, and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats.

§ 105.235 Communications.

(a) The Facility Security Officer must have a means to effectively notify facility personnel of changes in security conditions at the facility.

(b) Communication systems and procedures must allow effective and continuous communications between the facility security personnel, vessels interfacing with the facility, the cognizant COTP, and national and local authorities with security responsibilities.

(c) At each active facility access point, provide a means of contacting police, security control, or an emergency operations center, by telephones, cellular phones, and/or portable radios, or other equivalent means.

(d) Facility communications systems must have a backup means for both internal and external communications.

§ 105.240 Procedures for interfacing with vessels.

The facility owner or operator must ensure that there are measures for interfacing with vessels at all MARSEC Levels.

§ 105.245 Declaration of Security (DoS).

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

(b) At MARSEC Level 1, a facility receiving a cruise ship or a manned vessel carrying Certain Dangerous Cargo, in bulk, must comply with the following:

(1) Prior to the arrival of a vessel to the facility, the Facility Security Officer (FSO) and Master, Vessel Security Officer (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; and

(2) Upon the arrival of the vessel at the facility, the FSO and Master, VSO, or their designated representative, must sign the written DoS.

(c) Neither the facility nor the vessel may embark or disembark passengers, nor transfer cargo or vessel stores until the DoS has been signed and implemented.

(d) At MARSEC Levels 2 and 3, the FSOs of facilities interfacing with manned vessels subject to part 104 of this subchapter must sign and implement DoSs.

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

(1) The DoS is valid for a 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 that contained in the DoS, the continuing DoS is void and a new DoS must be executed in accordance with this section.

(g) A copy of all currently valid continuing DoSs must be kept with the Facility Security Plan.

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

§ 105.250 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.

(b) Security systems must be regularly tested in accordance with the manufacturers' recommendations; noted deficiencies corrected promptly; and the results recorded as required in § 105.225 of this subpart.

(c) The FSP must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 105.255 Security measures for access control.

(a) General. The facility 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 the facility; and

(3) Control access to the facility.

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

(1) The locations where restrictions or prohibitions that prevent unauthorized access are applied for each MARSEC Level. Each location allowing means of access to the facility must be addressed;

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

(3) The means of identification required to allow access to the facility and for individuals and vehicles to remain on the facility without challenge are established; and

(4) The identification of the locations where persons, personal effects and vehicle screenings are to be conducted. The designated screening areas should be covered to provide for continuous operations regardless of the weather conditions.

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

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

(2) Is coordinated, when practicable, with identification systems of vessels that use the facility;

(3) Is updated regularly;

(4) Uses disciplinary measures to discourage abuse;

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

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

(d) The facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(e) MARSEC Level 1. The facility owner or operator must ensure the following security measures are implemented at the facility:

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

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

(i) Entering the facility 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 enter;

(3) Check the identification of any person seeking to enter the facility, including vessel passengers and crew, facility employees, vendors, personnel duly authorized by

the cognizant authority, and visitors. This check includes confirming the reason for entry 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 the facility if the person is unable or unwilling, upon the request of facility personnel, to establish his or her identity or to account for his or her presence. Any such incident must be reported in compliance with this part;

(5) Designate restricted areas and provide appropriate access controls for these areas;

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

(7) Deter unauthorized access to the facility and to designated restricted areas within the facility;

(8) Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel; and

(9) Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between the facility and a vessel.

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

(1) Increasing the frequency and detail of the screening of persons, baggage, and personal effects for dangerous substances and devices entering the facility;

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

(3) Assigning additional personnel to guard access points and patrol the perimeter of the facility to deter unauthorized access;

(4) Limiting the number of access points to the facility by closing and securing some access points and providing physical barriers to impede movement through the remaining access points;

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

(6) Deterring waterside access to the facility, which may include, using waterborne patrols to enhance security around the facility; or

(7) Screening vehicles and their contents for dangerous substances and devices at the rate specified for MARSEC Level 2 in the approved FSP.

(g) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These 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;

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

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

(5) Suspending access to the facility;

(6) Suspending cargo operations;

(7) Evacuating the facility;

(8) Restricting pedestrian or vehicular movement on the grounds of the facility; or

(9) Increasing security patrols within the facility.

§ 105.260 Security measures for restricted areas.

(a) General. The facility 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 in the facility;

(3) Protect the facility;

(4) Protect vessels using and serving the facility;

(5) Protect sensitive security areas within the facility;

(6) Protect security and surveillance equipment and systems; and

(7) Protect cargo and vessel stores from tampering.

(b) Designation of Restricted Areas. The facility owner or operator must ensure restricted areas are designated within the facility. They must also ensure that all restricted areas are clearly marked and indicate that

access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The facility owner or operator may also designate the entire facility as a restricted area. Restricted areas must include, as appropriate:

(1) Shore areas immediately adjacent to each vessel moored at the facility;

(2) Areas containing sensitive security information, including cargo documentation;

(3) Areas containing security and surveillance equipment and systems and their controls, and lighting system controls; and

(4) Areas containing critical facility infrastructure, including:

(i) Water supplies;

(ii) Telecommunications;

(iii) Electrical system; and

(iv) Access points for ventilation and air-conditioning systems;

(5) Manufacturing or processing areas and control rooms;

(6) Locations in the facility where access by vehicles and personnel should be restricted;

(7) Areas designated for loading, unloading or storage of cargo and stores; and

(8) Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes.

(c) The owner or operator must ensure that all restricted areas have clearly established security measures to:

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

(2) Determine which persons other than facility 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;

(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;

(7) Control the entry, parking, loading and unloading of vehicles;

(8) Control the movement and storage of cargo and vessel stores; and

(9) Control unaccompanied baggage or personal effects.

(d) MARSEC Level 1. At MARSEC Level 1, the facility 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) Restricting access to only authorized personnel;

(2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;

(3) Assigning personnel to control access to restricted areas;

(4) Verifying the identification and authorization of all persons and all vehicles seeking entry;

(5) Patrolling or monitoring the perimeter of restricted areas;

(6) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry or movement within restricted areas;

(7) Directing the parking, loading, and unloading of vehicles within a restricted area;

(8) Controlling unaccompanied baggage and or personal effects after screening;

(9) Designating restricted areas for performing inspections of cargo and vessel stores while awaiting loading; and

(10) Designating temporary restricted areas to accommodate facility operations. If temporary restricted areas are designated, the FSP must include a requirement to conduct a security sweep of the designated temporary restricted area both before and after the area has been established.

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

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

(2) Enhancing the effectiveness of the barriers or fencing surrounding restricted areas, by the use of patrols or automatic intrusion detection devices;

(3) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;

(4) Restricting parking adjacent to vessels;

(5) Further restricting access to the restricted areas and movements and storage within them;

(6) Using continuously monitored and recorded surveillance equipment;

(7) Enhancing the number and frequency of patrols, including waterborne patrols undertaken on the boundaries of the restricted areas and within the areas; or

(8) Establishing and restricting access to areas adjacent to the restricted areas.

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

(1) Restricting access to additional areas;

(2) Prohibiting access to restricted areas, or

(3) Searching restricted areas as part of a security sweep of all or part of the facility.

§ 105.265 Security measures for handling cargo.

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

(1) Deter tampering;

(2) Prevent cargo that is not meant for carriage from being accepted and stored at the facility;

(3) Identify cargo that is approved for loading onto vessels interfacing with the facility;

(4) Include cargo control procedures at access points to the facility;

(5) Identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up;

(6) Restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate;

(7) Ensure the release of cargo only to the carrier specified in the cargo documentation;

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

(9) Create, update, and maintain a continuous inventory, including location, of all dangerous goods or

hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods or hazardous substances; and

(10) Be able to check cargo entering the facility for dangerous substances and devices at the rate specified in the approved Facility Security Plan (FSP). Means to check cargo include:

- (i) Visual examination;
- (ii) Physical examination;
- (iii) Detection devices, such as scanners; or
- (iv) Canines.

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

(1) Routinely check cargo, cargo transport units, and cargo storage areas within the facility prior to, and during, cargo handling operations to deter tampering;

(2) Check that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation;

(3) Screen vehicles; and

(4) Check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility.

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

(1) Conducting check of cargo, containers or other cargo transport units, and cargo storage areas within the port facility for dangerous substances and devices to the facility and vessel;

(2) Intensifying checks, as appropriate, to ensure that only the documented cargo enters the facility, is temporarily stored there, and then loaded onto the vessel;

(3) Intensifying the screening of vehicles;

(4) Increasing frequency and detail in checking of seals and other methods used to prevent tampering;

(5) Segregating inbound cargo, outbound cargo, and vessel stores;

(6) Increasing the frequency and intensity of visual and physical inspections; or

(7) Limiting the number of locations where dangerous goods and hazardous substances, including certain dangerous cargoes, can be stored.

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

(1) Restricting or suspending cargo movements or operations within all or part of the facility or specific vessels;

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

(3) Verifying the inventory and location of any dangerous goods and hazardous substances, including certain dangerous cargoes, held within the facility and their location.

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

(a) General. The facility 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;

(4) For vessels that routinely use a facility, establish and execute standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation; and

(5) Check vessel stores by the following means:

(i) Visual examination;

(ii) Physical examination;

(iii) Detection devices, such as scanners; or

(iv) Canines.

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

(1) Screen vessel stores at the rate specified in the approved Facility Security Plan (FSP);

(2) Require advance notification of vessel stores or bunkers delivery, including a list of stores, delivery vehicle driver information, and vehicle registration information;

(3) Screen delivery vehicles at the frequencies specified in the approved FSP; and

(4) Escort delivery vehicles within the facility at the rate specified by the approved FSP.

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

- (1) Detailed screening of vessel stores;
- (2) Detailed screening of all delivery vehicles;
- (3) Coordinating with vessel personnel to check the order against the delivery note prior to entry to the facility;
- (4) Ensuring delivery vehicles are escorted within the facility; or
- (5) Restricting or prohibiting the entry of vessel stores that will not leave the facility within a specified period.

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

- (1) Checking all vessel stores more extensively;

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

(3) Refusing to accept vessel stores on the facility.

§ 105.275 Security measures for monitoring.

(a) General. The facility owner or operator must ensure the implementation of security measures in this section and have the capability to continuously monitor, through a combination of lighting, security guards, waterborne patrols, and automatic intrusion-detection devices, or surveillance equipment, as specified in the approved Facility Security Plan (FSP), the:

(1) Facility and its approaches, on land and water;

(2) Restricted areas within the facility; and

(3) Vessels at the facility and areas surrounding the vessels.

(b) MARSEC Level 1. At MARSEC Level 1, the facility owner or operator must ensure the security measures in this section are implemented at all times, including the period from sunset to sunrise and periods of limited visibility.

For each facility, ensure monitoring capability that:

(1) When automatic intrusion-detection devices are used, activates an audible or visual alarm, or both, at a location that is continuously attended or monitored;

(2) Is able to function continually, including consideration of the possible effects of weather or of a power disruption;

(3) Monitors the facility area, including shore and waterside access to it;

(4) Monitors access points, barriers and restricted areas;

(5) Monitors access and movements adjacent to vessels using the facility, including augmentation of lighting provided by the vessel itself; and

(6) Limits lighting effects, such as glare, and their impact on safety, navigation, and other security activities.

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

(1) Increasing the coverage and intensity of surveillance equipment, including the provision of additional surveillance coverage;

(2) Increasing the frequency of foot, vehicle or waterborne patrols;

(3) Assigning additional security personnel to monitor and patrol; or

(4) Increasing the coverage and intensity of lighting, including the provision of additional lighting and coverage.

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

(1) Switching on all lighting within, or illuminating the vicinity of, the facility;

(2) Switching on all surveillance equipment capable of recording activities within or adjacent to the facility;

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

(4) Complying with the instructions issued by those responding to the security incident.

§ 105.280 Security incident procedures.

For each MARSEC Level, the facility owner or operator must ensure the Facility Security Officer and facility security personnel are able to:

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

(b) Evacuate the facility in case of security threats or breaches of security;

(c) Report security incidents as required in § 101.305 of this subchapter;

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

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

§ 105.285 Additional requirements—passenger and ferry facilities.

(a) At MARSEC Level 1, the owner or operator of a passenger or ferry facility must ensure, in coordination with a vessel moored at the facility, that the following security measures are implemented in addition to the requirements of this part:

(1) In a facility with no public access area designated under § 105.106, establish separate areas to segregate unchecked persons and personal effects from checked persons and personal effects;

(2) Ensure that a defined percentage of vehicles to be loaded aboard are screened prior to loading, in accordance with a MARSEC Directive or other orders issued by the Coast Guard;

(3) Ensure that all unaccompanied vehicles to be loaded on passenger vessels are screened prior to loading;

(4) Deny passenger access to restricted areas unless supervised by facility security personnel; and

(5) In a facility with a public access area designated under § 105.106, provide sufficient security personnel to monitor all persons within the area and conduct screening of persons and personal effects, as needed.

(b) At MARSEC Level 2, in addition to the requirements for MARSEC Level 1, the owner or operator of a passenger or ferry facility with no public access area designated under § 105.106 must ensure screening of additional passengers, baggage, and vehicles prior to boarding the vessel as specified in the approved FSP and Declaration of Security.

(c) At MARSEC Level 3, in addition to the requirements for MARSEC Level 1 and MARSEC Level 2 and in coordination with the vessel moored at the facility, the owner or operator of a passenger or ferry facility with no

public access area designated under § 105.106 must ensure the following security measures:

- (1) Screen and identify all persons;
- (2) Screen all baggage; and
- (3) Assign additional security personnel and patrols.

§ 105.290 Additional requirements—cruise ship terminals.

At all MARSEC Levels, in coordination with a vessel moored at the facility, the facility owner or operator must ensure the following security measures:

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

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

(c) Designate holding, waiting, or embarkation areas to segregate screened persons and their personal effects awaiting embarkation from unscreened persons and their personal effects;

(d) Provide additional security personnel to designated holding, waiting, or embarkation areas; and

(e) Deny passenger access to restricted areas unless supervised by facility security personnel.

§ 105.295 Additional requirements—Certain Dangerous Cargo (CDC) facilities.

(a) At all MARSEC Levels, owners or operators of CDC facilities must ensure the implementation of the following security measures in addition to the requirements of this part:

(1) Escort all visitors, contractors, vendors, and other non-facility employees at all times while on the facility, if access identification is not provided. Escort provisions do not apply to prearranged cargo deliveries;

(2) Control the parking, loading, and unloading of vehicles within a facility;

(3) Require security personnel to record or report their presence at key points during their patrols;

(4) Search unmanned or unmonitored waterfront areas for dangerous substances and devices prior to a vessel's arrival at the facility; and

(5) Provide an alternate or independent power source for security and communications systems.

(b) At MARSEC Level 2, in addition to the requirements for MARSEC Level 1, owners or operators of CDC facilities must ensure the implementation of the following security measures:

(1) Release cargo only in the presence of the Facility Security Officer (FSO) or a designated representative of the FSO; and

(2) Continuously guard or patrol restricted areas.

(c) At MARSEC Level 3, in addition to the requirements for MARSEC Level 1 and MARSEC Level 2, owners or operators of CDC facilities must ensure the facilities are continuously guarded and restricted areas are patrolled.

§ 105.296 Additional requirements—barge fleeting facilities.

(a) At MARSEC Level 1, in addition to the requirements of this part, an owner or operator of a barge fleeting facility must ensure the implementation of the following security measures:

(1) Designate an area within the fleeting facility to segregate those barges carrying Certain Dangerous Cargoes and cargoes listed in 46 CFR, subchapter D and O of chapter I, title 46, Code of Federal Regulations or Certain Dangerous Cargoes from all other barges in the fleeting facility;

(2) Maintain a current list of vessels and cargoes in the designated restricted area; and

(3) Ensure that at least one towing vessel is available to service the fleeting facility for every 100 barges within the facility.

(b) At MARSEC Level 2, in addition to the requirements of this part and MARSEC Level 1 requirements, an owner or operator of a barge fleeting facility must ensure security personnel are assigned to monitor or patrol the designated restricted area within the barge fleeting facility.

(c) At MARSEC Level 3, in addition to the requirements of this part and MARSEC Level 2 requirements, an owner or operator of a barge fleeting facility must ensure that both land and waterside perimeters of the designated restricted area within the barge fleeting facility are continuously monitored or patrolled.

Subpart C—Facility Security Assessment (FSA)

§ 105.300 General.

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

(b) A common FSA may be conducted for more than one similar facility provided the FSA reflects any facility-specific characteristics that are unique.

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

(d) Those involved in a FSA must be able to draw upon expert assistance in the following areas, as appropriate:

- (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 structures and facility services;
- (7) Facility security requirements;
- (8) Facility and vessel 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 or civil engineering; and

(13) Facility and vessel operations.

§ 105.305 Facility Security Assessment (FSA) requirements.

(a) Background. The facility owner or operator must ensure that the following background information, if applicable, is provided to the person or persons who will conduct the assessment:

(1) The general layout of the facility, including:

(i) The location of each active and inactive access point to the facility;

(ii) The number, reliability, and security duties of facility personnel;

(iii) Security doors, barriers, and lighting;

(iv) The location of restricted areas;

(v) The emergency and stand-by equipment available to maintain essential services;

(vi) The maintenance equipment, cargo spaces, storage areas, and unaccompanied baggage storage;

(vii) Location of escape and evacuation routes and assembly stations; and

(viii) Existing security and safety equipment for protection of personnel and visitors;

(2) Response procedures for fire or other emergency conditions;

(3) Procedures for monitoring facility and vessel personnel, vendors, repair technicians, and dock workers;

(4) Existing contracts with private security companies and existing agreements with local or municipal agencies;

(5) Procedures for controlling keys and other access prevention systems;

(6) Procedures for cargo and vessel stores operations;

(7) Response capability to security incidents;

(8) Threat assessments, including the purpose and methodology of the assessment, for the port in which the facility is located or at which passengers embark or disembark;

(9) Previous reports on security needs; and

(10) Any other existing security procedures and systems, equipment, communications, and facility personnel.

(b) On-scene survey. The facility owner or operator must ensure that an on-scene survey of each facility is conducted. The on-scene survey examines and evaluates existing facility protective measures, procedures, and

operations to verify or collect the information required in paragraph (a) of this section.

(c) Analysis and recommendations. In conducting the FSA, the facility owner or operator must ensure that the FSO analyzes the facility background information and the on-scene survey, and considering the requirements of this part, provides recommendations to establish and prioritize the security measures that should be included in the FSP. The analysis must consider:

(1) Each vulnerability found during the on-scene survey including but not limited to:

(i) Waterside and shore-side access to the facility and vessel berthing at the facility;

(ii) Structural integrity of the piers, facilities, and associated structures;

(iii) Existing security measures and procedures, including identification systems;

(iv) Existing security measures and procedures relating to services and utilities;

(v) Measures to protect radio and telecommunication equipment, including computer systems and networks;

(vi) Adjacent areas that may be exploited during or for an attack;

(vii) Areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the facility;

(viii) Existing agreements with private security companies providing waterside and shore-side security services;

(ix) Any conflicting policies between safety and security measures and procedures;

(x) Any conflicting facility operations and security duty assignments;

(xi) Any enforcement and personnel constraints;

(xii) Any deficiencies identified during daily operations or training and drills; and

(xiii) Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits;

(2) Possible security threats, including but not limited to:

(i) Damage to or destruction of the facility or of a vessel moored at the facility;

(ii) Hijacking or seizure of a vessel moored at the facility or of persons on board;

(iii) Tampering with cargo, essential equipment or systems, or stores of a vessel moored at the facility;

- (iv) Unauthorized access or use including the presence of stowaways;
- (v) Smuggling dangerous substances and devices to the facility;
- (vi) Use of a vessel moored at the facility to carry those intending to cause a security incident and their equipment;
- (vii) Use of a vessel moored at the facility as a weapon or as a means to cause damage or destruction;
- (viii) Blockage of entrances, locks, and approaches;
and
- (ix) Nuclear, biological, radiological, explosive, and chemical attack;
- (3) Threat assessments by Government agencies;
- (4) Vulnerabilities, including human factors, in the facility's infrastructure, policies and procedures;
- (5) Any particular aspects of the facility, including the vessels using the facility, which make it likely to be the target of an attack;
- (6) Likely consequences in terms of loss of life, damage to property, and economic disruption, including disruption to transportation systems, of an attack on or at the facility; and

(7) Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

(d) FSA report.

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

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

(ii) A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;

(iii) A description of each vulnerability found during the on-scene survey;

(iv) A description of security measures that could be used to address each vulnerability;

(v) A list of the key facility operations that are important to protect; and

(vi) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the facility.

(2) A FSA report must describe the following elements within the facility:

(i) Physical security;

- (ii) Structural integrity;
- (iii) Personnel protection systems;
- (iv) Procedural policies;
- (v) Radio and telecommunication systems, including computer systems and networks;
- (vi) Relevant transportation infrastructure; and
- (vii) Utilities.

§ 105.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan required in § 105.415 of this part.

(b) A facility owner or operator may generate and submit a report that contains the Facility Security Assessment for more than one facility subject to this part, to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP.

Subpart D—Facility Security Plan (FSP)

§ 105.400 General.

(a) The Facility Security Officer (FSO) must ensure a Facility Security Plan (FSP) is developed and implemented for each facility for which he or she is designated as FSO. The FSP:

- (1) Must identify the FSO by name and position, and provide 24-hour contact information;
- (2) Must be written in English;
- (3) Must address each vulnerability identified in the Facility Security Assessment (FSA);
- (4) Must describe security measures for each MARSEC Level; and
- (5) May cover more than one facility to the extent that they share similarities in design and operations, if authorized and approved by the cognizant COTP.

(b) The FSP must be submitted for approval to the cognizant COTP in a written or electronic format. Format for submitting the FSP electronically can be found at <http://www.uscg.mil/HQ/MSC>.

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

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

§ 105.405 Format and content of the Facility Security Plan (FSP).

(a) A facility owner or operator must ensure that the FSP consists of the individual sections listed in this paragraph (a). If the FSP does not follow the order as it

appears in the list, the facility owner or operator must ensure that the FSP contains an index identifying the location of each of the following sections:

- (1) Security administration and organization of the facility;
- (2) Personnel training;
- (3) Drills and exercises;
- (4) Records and documentation;
- (5) Response to change in MARSEC Level;
- (6) Procedures for interfacing with vessels;
- (7) Declaration of Security (DoS);
- (8) Communications;
- (9) Security systems and equipment maintenance;
- (10) Security measures for access control, including designated public access areas;
- (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 security plan amendments;
- (17) Facility Security Assessment (FSA) report; and

(18) Facility Vulnerability and Security Measures Summary (Form CG-6025) in appendix A to part 105—Facility Vulnerability and Security Measures Summary (CG-6025).

(b) The facility owner or operator must ensure that the FSP describes in detail how each of the individual requirements of subpart B of this part will be met.

(c) The Facility Vulnerability and Security Measures Summary (Form CG-6025) must be completed using information in the FSA concerning identified vulnerabilities and information in the FSP concerning security measures in mitigation of these vulnerabilities.

§ 105.410 Submission and approval.

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

(1) Submit one copy of their Facility Security Plan (FSP) for review and approval to the cognizant COTP; or

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

(b) Facilities constructed 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 cognizant COTP 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) An FSP may be submitted and approved to cover more than one facility where they share similarities in design and operations, if authorized and approved by the cognizant COTP.

(e) Each facility owner or operator that submits one FSP to cover two or more facilities of similar design and operation must address facility-specific information that includes the design and operational characteristics of each facility and must complete a separate Facility Vulnerability and Security Measures Summary (Form CG-6025), in appendix A to part 105—Facility Vulnerability and Security Measures Summary (CG-6025), for each facility covered by the plan.

(f) A FSP that is approved by the cognizant COTP is valid for five years from the date of its approval.

§ 105.415 Amendment and audit.

(a) Amendments.--

(1) Amendments to a FSP that is approved by the cognizant COTP may be initiated by:

(i) The facility owner or operator; or

(ii) The cognizant COTP upon a determination that an amendment is needed to maintain the facility's security.

The cognizant COTP, who will give the facility owner or operator written notice and request that the facility owner or operator propose amendments addressing any matters specified in the notice. The facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the COTP.

(2) Proposed amendments must be submitted to the cognizant COTP. If initiated by the facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant COTP allows a shorter period. The cognizant COTP will approve or disapprove the proposed amendment in accordance with § 105.415 of this subpart.

(3) If there is a change in the owner or operator, the Facility Security Officer (FSO) must amend the Facility Security Plan (FSP) to include the name and contact information of the new facility owner or operator and

submit the affected portion of the FSP for review and approval in accordance with § 105.415 if this subpart.

(b) Audits.--

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

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

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

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

(i) Have knowledge of methods for conducting audits and inspections, and security, 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 FSA or FSP, the FSO must submit, in accordance with § 105.415 of this subpart, the amendments to the cognizant COTP for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets the applicable requirements of this part.

Appendix A to part 105—Facility Vulnerability and Security Measures Summary (Form CG-6025).

INSTRUCTIONS FOR THE CG-6025 FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY

This form satisfies the requirements for Facility Vulnerability and Security Measures Summary submission found in the Code of Federal Regulations for Facility Security. Form CG-6025A, Vulnerability and Security Measures Addendum, may be used as a continuation of form CG-6025, in order to submit additional vulnerabilities and security measures. If a facility owner or operator submits a Facility Vulnerability and Security Measures Summary pertaining to more than one facility, form CG-6025, shall be submitted to document each additional facility.

BLOCK 1	Self-Explanatory.	BLOCK 8b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 2	Street Address.		
BLOCK 3	If available, provide latitude to nearest tenth of a minute.		
BLOCK 4	If available, provide longitude to nearest tenth of a minute.	BLOCK 9a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 2 that will mitigate the vulnerability you addressed.
BLOCK 5	Provide the Captain of the Port Zone from the list below in which your facility resides. Their respective zones are described in 33 CFR Part 3.		
BLOCK 6	Check all applicable operations that are conducted at your facility. If you select other, please explain in the box provided.	BLOCK 9b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 7a	Enter a concise description of a vulnerability identified in your facility's assessment. Provide location information if appropriate.	BLOCK 10a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 3 that will mitigate the vulnerability you addressed.
BLOCK 7b	Enter the vulnerability identification code from the KEY to categorically identify the vulnerability you described. More than one category may be used. If you select other, please explain in the box provided.		
BLOCK 8a	Enter a concise description of a selected security measure identified in the plan for MARSEC Level 1 that will mitigate the vulnerability you addressed.	BLOCK 10b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.

CAPTAIN OF THE PORT ZONE:

Anchorage	Honolulu	Mobile	Puget Sound
Baltimore	Houston-Galveston	Morgan City	San Diego
Boston	Huntington	New Orleans	San Francisco
Buffalo	Jacksonville	New York	San Juan
Charleston	Juneau	Paducah	Sault Ste. Marie
Chicago	Long Island Sound	Philadelphia	Savannah
Cleveland	Los Angeles/Long Beach	Pittsburgh	St. Louis
Corpus Christi	Louisville	Port Arthur	Tampa
Detroit	Memphis	Portland, ME	Toledo
Duluth	Miami	Portland, OR	Valdez
Guam	Milwaukee	Providence	Wilmington
Hampton Roads			

KEY

VULNERABILITY CATEGORY:

Physical Security	PHS	That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against terrorism, espionage, sabotage, damage, and theft.
Structural Integrity	STI	The design and material construction characteristics of piers, facilities, and associated structures.
Transportation Infrastructure	TRI	Infrastructure that may be exploited during an attack, other than utilities.
Utilities	UTI	The essential equipment and services that are vital to the operation of the facility.
Radio & Telecommunications	RAT	That part of security concerned with measures to protect radio and telecommunication equipment, including computer systems and networks.
Personnel Protection Systems	PPS	Equipment, Gear, or Systems designed to protect facility personnel (i.e. weapons, body armor).
Procedural Policies	PRP	Plans, Policies, and Procedures for specific operations.
Coordination and Information Sharing	CIS	The ability to coordinate and receive/share information with local/state/federal agencies and other commercial entities.
Preparedness	PRE	Implementation of Plans, Policies, and Procedures through Training, Drills, and Exercises conducted to improve security awareness, prevention, and response.

SECURITY MEASURES

Access Control	ACC	Lighting	LIT
Barriers	BAR	Patrols	PAT
Cargo Control	CAC	Planning, Policies, & Procedures	PPP
Communications	COM	Redundancy	RED
Coordination	COR	Response	RES
Credentialing	CRE	Stand-off Distance	SOD
Detection	DET	Structural Hardening	STH
Guard Force	GUF	Surveillance	SUR
IT Security	ITS	Training	TRA
Inspections	INS	Vessels/Vehicles	VEV
Intelligence	INT		

FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY

An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB

1. Name of Facility

2. Address of Facility

3. Latitude

4. Longitude

5. Captain of the Port Zone

6. Type of Operation (check all that apply)

- If other, explain
 Petroleum
 Certain Dangerous Cargo
 Passengers (Subchapter H)
- If other, explain below:
- Dry Bulk
 Chemical
 Barge Fleeting
 Passengers (Ferries)
- Container
 LHG/LNG
 Offshore Support
 Passengers (Subchapter K)

7a. Vulnerability

7b. Vulnerability Category

If other, explain

8a. Selected Security Measures (MARSEC Level 1)

8b. Security Measures Category??

If other, explain

9a. Selected Security Measures (MARSEC Level 2)

9b. Security Measures Category

If other, explain

10a. Selected Security Measures (MARSEC Level 3)

10b. Security Measures Category

If other, explain

7a. Vulnerability

7b. Vulnerability Category

If other, explain

8a. Selected Security Measures (MARSEC Level 1)

8b. Security Measures Category

If other, explain

9a. Selected Security Measures (MARSEC Level 2??)

9b. Security Measures Category

If other, explain

10a. Selected Security Measures (MARSEC Level 3)

10b. Security Measures Category

If other, explain

VULNERABILITY AND SECURITY MEASURES ADDENDUM

An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB

NAME OF FACILITY (Use same Name as Block 1., of CG-6025)

7a. Vulnerability

7b. Vulnerability Category

If other, explain

8a. Selected Security Measures (MARSEC Level 1)

8b. Security Measures Category

If other, explain

9a. Selected Security Measures (MARSEC Level 2)

9b. Security Measures Category

If other, explain

10a. Selected Security Measures (MARSEC Level 3)

10b. Security Measures Category

If other, explain

7a. Vulnerability

7b. Vulnerability Category

If other, explain

8a. Selected Security Measures (MARSEC Level 1)

8b. Security Measures Category

If other, explain

9a. Selected Security Measures (MARSEC Level 2)

9b. Security Measures Category

If other, explain

10a. Selected Security Measures (MARSEC Level 3)

10b. Security Measures Category

If other, explain

7a. Vulnerability

7b. Vulnerability Category

If other, explain

8a. Selected Security Measures (MARSEC Level 1)

8b. Security Measures Category

If other, explain

9a. Selected Security Measures (MARSEC Level 2)

9b. Security Measures Category

If other, explain

10a. Selected Security Measures (MARSEC Level 3)

10b. Security Measures Category

If other, explain