Overview of Facility Security Regulations

33 CFR Part 105

U.S. COAST GUARD

October 2003

NOTE: Bold type indicates a change from the interim rules.

Application

The rulemaking applies to:

- facilities subject to 33 CFR parts 126, 127, and 154;
- facilities that receive vessels certified to carry more than 150 passengers, **except those vessels not carrying and not embarking or disembarking passengers at the facility**;
- facilities that receive vessels on international voyages, including vessels solely navigating the Great Lakes;
- **facilities that receive vessels subject to the International Convention for the Safety of Life at Sea, 1974, chapter XI;**
- **facilities that receive U.S. cargo vessels greater than 100 gross register tons;**
- **facilities that receive U.S. cargo vessels, greater than 100 gross register tons, subject to 46 CFR chapter 1, subchapter 1, except for those facilities that receive only commercial fishing vessels inspected under 46 CFR part 105; or**
- **barge fleeting facilities that receive barges carrying in bulk, cargoes regulated by 46 CFR chapter 1, subchapters D or O, or Certain Dangerous Cargoes.**

The U.S. Coast Guard will verify that these facilities comply with the security rules through inspections.

In the final rules three types of facilities were exempted including those that only service passenger vessels when those vessels are not carrying passengers, public access facilities that are used by the public primarily for purposes such as recreation, entertainment, retail, or tourism, and shipyards.

Waivers

The regulations detail the procedures for requesting a waiver for the benefit of facility owners or operators who find specific requirements of the rulemaking unnecessary.

(There were no changes in the final rule to this section)

Equivalents

The equivalents section of the regulations 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.

(There were no changes in the final rule to this section)

Alternative Security Program

The Coast Guard will allow owners or operators of facilities to implement an Alternative Security Program (ASP) 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 security assessments to demonstrate they meet the intent of each section of these requirements. The program must be implemented in its entirety and is valid for five years.

If a facility is intending to operate under an ASP, the facility owner or operator must send a signed letter to the Captain of the Port stating which approved ASP program the facility is intending to use by the December 31, 2003, deadline for security plans.

In the final rules, the USCG has allowed more flexibility for non-SOLAS vessels and all facilities to participate in an ASP, if they wish. This program was strongly endorsed by several organizations because it allows security measures to be tailored to the unique needs of each industry segment. A facility can develop an ASP on their own, work collectively with other similar facilities to develop an ASP or use an established ASP providing that it is approved by the COTP for use by that facility.

The USCG approved a number of ASPs which may be used by vessel or facility owners or operators to meet the provisions of the regulations. These include: the American Gaming Association Alternative Security Program, the American Waterways Operators Alternative Security Program for Tugboats, Towboats and Barges, and the Passenger Vessel Association Industry Standards for Security of Passenger Vessels and Small Passenger Vessels.

Evaluating Submissions of Waivers, Equivalents, and Alternative Security Programs

In the Coast Guard's evaluation of waivers, equivalencies, and Alternative Security Programs, they 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 alternative is at least as effective as that intended by the interim rule.

(There were no changes in the final rule to this section.)

Facility Owner or Operator Responsibilities

Each facility owner or operator must develop an effective security plan that incorporates detailed preparation, prevention, and response activities for each MARSEC Level, and detail the organi-

zations or personnel responsible for carrying out those activities. These requirements are consistent with the International Ship and Port Facility Security Code (ISPS).

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;
- 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;
- **Ensuring security for unattended vessels moored at the facility; and**
- **Ensuring consistency between security and safety requirements.**

In comments submitted to the USCG, AAPA asked for a clarification of the definition of facility owner or operator. The Coast Guard defines owner or operator as "any person or entity that maintains operational control over any facility, vessel, or OSC facility subject to the requirements of this subchapter." AAPA requested that operational control be further defined as "the ability to influence or control the physical or commercial activities pertaining to that facility for any period of time." **The USCG did not accept this clarification on the grounds that our definition does not provide for security activities in addition to physical or commercial activities.**

Facility Security Officer (FSO)

The facility owner or operator must designate in writing a Facility Security Officer for each facility. This person may be a full-time or collateral duty position. The FSO 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 of the FSO 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 FSO may assign security duties to other facility personnel; however, the FSO remains responsible for these duties.

(No significant changes in the final rule.)

Training

Required training for facility personnel must be specified in the Facility Security Plan (FSP). Specific security training courses for the FSO and facility personnel will not be required by the Coast Guard. While formal training may be appropriate, specifics are not being mandated. Facility owners or operators must certify that security personnel are, in fact, properly trained to perform their duties. The FSO is required to ensure that facility security persons possess necessary training to maintain the overall security of the facility.

In the final rules, training for non-security personnel was modified to be more flexible to the employee's position within the port. These employees may not need to be trained in all areas.

Drill and Exercise Requirements

Exercises are required to ensure the adequacy of the FSP and must 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 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.

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

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.

(There were no changes in the final rule to this section.)

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:

- Access control;
- Restricted areas;
- Handling cargo;
- Delivery of vessel stores and bunkers; and
- Monitoring.

(There were no changes in the final rule to this section.)

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.

(There were no changes in the final rule to this section.)

Declaration of Security (DOS)

This 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 DOS 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 DOS for every evolution regardless of the MARSEC Level. At MARSEC Levels 2 and 3, all vessels and facilities would need to complete the DOS. **The facility owner or operator (the facility security officer or their designated representatives of the facility) must ensure procedures are established for requesting and implementing a DOS at MARSEC Levels 2 and 3.**

Facilities that frequently receive the same vessel may execute a single DOS for multiple visits. Every DOS must state the security activities for which the facility and vessel are responsible during vessel-to-facility interfaces.

AAPA stated in comments to the USCG that facilities must have the ability to exchange the DOS electronically. The exchange of a DOS in paper form is inefficient, could cause delays for certain operations, and would require significant personnel resources. This was not addressed in the final rule.

Facility Security Assessment (FSA)

All regulated facilities (identified above) must complete a Facility Security Assessment (FSA), which is an essential and integral part of the process of developing and updating the required Facility Security Plan (FSP) — based on the results of the FSA. The Facility Security Officer must examine and evaluate existing facility protective measures, procedures, and operations.

The FSO must also examine each identified point of access, including rail access, roads, water-side, and gates, and evaluate its potential for use by individuals with legitimate access, as well as those seeking unauthorized entry.

Each facility owner or operator is required to document and retain its FSA for a period of five years and must include it as an appendix in the FSP. Prior to conducting an FSA, the FSO 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. Step one of the facility 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. Then the vulnerabilities must be prioritized and entered into the Facility Security Plan. The assessment must be updated every five years or when the FSP is updated.

This section included only a few clarifications. **Most significantly a new addition under part 105.305 (d)(3) requires the FSA report to list the persons, activities, services and operations that are important to protect and a listing of those areas.**

Facility Security Plan (FSP)

The USCG requirements for plans are consistent with the ISPS Code. FSPs must incorporate the results of the required FSA and consider the recommended measures appropriate to each facility. FSPs can be combined with or complement existing safety management systems. The plans may be kept in a protected electronic format. The plans must also be protected from unauthorized access or disclosure.

FSPs 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, 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 FSP and for updating it;
- Documented procedures for reporting security incidents;
- Written designation of the FSO;
- 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 found in the Federal Register notice on Facility Security).

(There were no significant changes to this section.)

Submission and Approval of Security Plan

The Facility Security Plan, including the Facility Security Assessment report and Facility Vulnerability and Security Measures Summary (Form CG-6025), must be submitted to the cognizant COTP by **December 31, 2003**. Once the COTP finds that the plan meets the security requirements in 33 CFR 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 FSP, the cognizant COTP may return to the submitter a written acknowledgement 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.

If the COTP finds that the FSP 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 USCG every time:

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

USCG made a few modifications to the submission requirements including that the facility owner or operator must either:

- **Submit one copy of their FSP for review and approval to the cognizant COTP and a letter certifying that the FSP meets applicable requirements of this part; or**
- **If intending to operate under an Approved Security Program, a letter signed by the facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use;**

Owners or operators of facilities not in service on or before December 31, 2003, must comply with the requirements above 60 days prior to beginning operations or by December 31, 2003, whichever is later.

In comments submitted to the USCG, AAPA asked that procedures be developed for how the COTP approves plans so there is consistency from port to port. This issue was not addressed by the USCG in the final rule, however, the Coast Guard has agreed to provide guidance for developing assessments and plans.

Link to regulations: http://www.aapa-ports.org/govrelations/uscg_final_regs.htm

American Association of Port Authorities
Serving the Ports of Canada, the Caribbean, Latin America and the United States

AMERICAN ASSOCIATION OF PORT AUTHORITIES
1010 Duke Street -- Alexandria, VA 22314 – (703) 684-5700