

## § 104.267

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

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

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

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

(iii) Refuse to accept unaccompanied baggage on board;

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

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

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

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

(7) Suspending cargo operations;

(8) Evacuating the vessel;

(9) Moving the vessel; or

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

[USCG-2006-24196, 72 FR 3580, Jan. 25, 2007]

### § 104.267 Security measures for newly hired employees.

(a) Newly-hired vessel employees may be granted entry to secure areas of the vessel for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements in paragraph (b) of this section are met, and provided that the new hire is accompanied by an individual with a TWIC while within the secure areas of the vessel. If TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend access to secure areas for another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. The Coast Guard will issue guidance for use in making these determinations.

(b) Newly-hired vessel employees may be granted the access provided for in paragraph (a) of this section only if:

(1) The new hire has applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process, paying the user fee, and is not currently engaged in a waiver or appeal

## 33 CFR Ch. I (7-1-10 Edition)

process. The vessel owner or operator or Vessel Security Officer (VSO) must have the new hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC;

(2) The vessel owner or operator or the VSO enters the following information on the new hire into the Coast Guard's Homeport website (<http://homeport.uscg.mil>):

(i) Full legal name, including middle name if one exists;

(ii) Date of birth;

(iii) Social security number (optional);

(iv) Employer name and 24 hour contact information; and

(v) Date of TWIC enrollment;

(3) The new hire presents an identification credential that meets the requirements of §101.515 of this subchapter;

(4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the vessel owner or operator or VSO have not been informed by the cognizant COTP that the new hire poses a security threat; and

(5) There would be an adverse impact to vessel operations if the new hire is not allowed access.

(c) This section does not apply to any individual being hired as a Company Security Officer (CSO) or VSO, or any individual being hired to perform vessel security duties.

(d) The new hire may not begin working on board the vessel under the provisions of this section until the owner, operator, or VSO receives notification, via Homeport or some other means, the new hire has passed an initial name check.

[USCG-2006-24196, 72 FR 3581, Jan. 25, 2007]

### § 104.270 Security measures for restricted areas.

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

(1) Prevent or deter unauthorized access;

(2) Protect persons authorized to be on board;

(3) Protect the vessel;

(4) Protect sensitive security areas within the vessel;

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

(6) Protect cargo and vessel stores from tampering.

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

(1) Navigation bridge, machinery spaces and other control stations;

(2) Spaces containing security and surveillance equipment and systems and their controls and lighting system controls;

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

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

(5) Spaces containing dangerous goods or hazardous substances;

(6) Spaces containing cargo pumps and their controls;

(7) Cargo spaces and spaces containing vessel stores;

(8) Crew accommodations; and

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

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

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

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

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

(4) Define the extent of any restricted area;

(5) Define the times when access restrictions apply; and

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

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

(1) Locking or securing access points;

(2) Monitoring and using surveillance equipment;

(3) Using guards or patrols; and

(4) Using automatic intrusion detection devices, which if used must activate an audible and/or visual alarm at a location that is continuously attended or monitored, to alert vessel personnel to unauthorized access.

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

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

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

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

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

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

(1) Restricting access to additional areas; and

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

**§ 104.275 Security measures for handling cargo.**

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

(1) Deter tampering;

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

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

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

(5) When there are regular or repeated cargo operations with the same