

access by land and patrolling the shoreline is impractical. One commenter stated that it would be very difficult to coordinate shore-side patrols when the facility owner does not own the land.

We recognize that it may be difficult to monitor or patrol remote barge fleeting facilities. However, we have determined that barge fleeting facilities may be involved in a transportation security incident if fleeting barges carry dangerous goods or hazardous substances. Section 105.296 does allow facility owners and operators to use monitoring in remote locations as an alternative to shore-side patrols.

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

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

Subpart C—Facility Security Assessment (FSA)

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

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

Sections 104.405, 105.405, and 106.405 require that the security assessment report be submitted with the respective security plans. We believe that the security assessment report must be submitted as part of the security plan approval process because it is used to determine if the security plan adequately addresses the security requirements of the regulations. The information provided in form CG-6025 will be used to assist in the development of AMS Plans. The security assessments are not required to be submitted. To clarify that the report, not the assessment, is what must be submitted with the Vessel or Facility Security Plan, we are amending § 104.305 to add the word "report" where appropriate. We have also amended §§ 105.305 and 106.305 for facilities and OCS facilities, respectively. Additionally, we have amended these sections so that the Facility Security Assessment report requirements mirror the Vessel Security Assessment report requirements. All of these requirements were included in our original submission to OMB for "Collection of Information" approval, and there is no associated increase in burden in our collection of information summary. We also acknowledge that security assessments and security assessment reports have sensitive security information within them, and that they should be protected from unauthorized access under §§ 104.400(c), 105.400(c), and 106.400(c). Therefore, we are amending §§ 104.305, 105.305, and 106.305 to clarify that all security assessments, security assessment reports, and security plans need to be protected from unauthorized disclosure. The Coast Guard has already instituted measures to protect sensitive security information, such as security assessment reports and security plans, from disclosure.

Ten commenters addressed the disclosure of security plan information. One commenter seemed to advocate making security plans public. One commenter was concerned that plans will be disclosed under the Freedom of Information Act (FOIA). One commenter requested that mariners and other employees whose normal working conditions are altered by a Vessel or Facility Security Plan be granted access to sensitive security information contained in that plan on a need-to-know basis. One commenter stated that Company Security Officers and Facility Security Officers should have reasonable access to AMS Plan information on a need-to-know basis. One commenter stated that the Federal

government must preempt State law in instances of sensitive security information because of past experience with State laws that require full disclosure of public documents. Three commenters supported our conclusion that the MTSA and our regulations preempt any conflicting State requirements. Another commenter is particularly pleased to observe the strong position taken by the Coast Guard in support of Federal preemption of possible State and local security regimes. One commenter supported our decision to designate security assessments and plans as sensitive security information.

Portions of security plans are sensitive security information and must be protected in accordance with 49 CFR part 1520. Only those persons specified in 49 CFR part 1520 will be given access to security plans. In accordance with 49 CFR part 1520 and pursuant to 5 U.S.C. 552(b)(3), sensitive security information is generally exempt from disclosure under FOIA, and TSA has concluded that State disclosure laws that conflict with 49 CFR part 1520 are preempted by that regulation. 46 U.S.C. 70103(d) also provides that the information developed under this regulation is not required to be disclosed to the public. However, §§ 104.220, 104.225, 105.210, 105.215, 106.215, and 106.220 of these rules state that vessel and facility personnel must have knowledge of relevant provisions of the security plan. Therefore, vessel and facility owners or operators will determine which provisions of the security plans are accessible to crewmembers and other personnel. Additionally, COTPs will determine what portions of the AMS Plan are accessible to Company or Facility Security Officers.

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

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

"Sensitive security information" is a designation mandated by regulations promulgated by TSA and may be found