

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 in 49 CFR part 1520. These regulations state that information designated as sensitive security information may not be shared with the general public. FOIA exempts from its mandatory release provisions those items that other laws forbid from public release. Thus, security assessments, security assessment reports, and security plans, which should be designated as sensitive security information, are all exempt from release under FOIA.

One commenter stated that the owners and operators of commercial vessels do not have the resources for additional work and paperwork requirements, believing that the rule will drive some owners and operators out of business.

The MTSA requires the owners or operators of vessels that may be

involved in a transportation security incident to develop and implement security plans for their vessels. While these regulations will result in an increased burden for much of the maritime industry, we believe the rules are necessary to ensure maritime homeland security. We have developed these regulations to be as flexible as possible in their implementation, including allowing Alternative Security Programs and equivalencies, while still ensuring maritime security.

Six commenters suggested that a template for security assessments and plans be provided for affected entities. One commenter specifically asked for guidance templates for barge fleeting facilities.

We intend to develop guidelines for the development of security assessments and plans. Additionally, the regulations allow owners and operators of facilities and vessels to implement Alternative Security Programs. This allows owners and operators to participate in a development process with other industry groups, associations, or organizations. We anticipate that one such Alternative Security Program will include a template for barge fleeting facilities.

We received four comments regarding the use of third party companies to conduct security assessments. Two commenters asked if we will provide a list of acceptable assessment companies because of the concern that the vulnerability assessment could "fall into the wrong hands." One commenter requested that the regulations define "appropriate skills" that a third party must have in order to aid in the development of security assessments. One commenter stated that the person or company conducting the assessment might not be reliable.

We will not be providing a list of acceptable assessment companies, nor will we define "appropriate skills." It is the responsibility of the vessel or facility owner or operator to vet companies that assist them in their security assessments. In the temporary interim rule (68 FR 39254) (part 101), we stated, "we reference ISPS Code, part B, paragraph 4.5, as a list of competencies all owners and operators should use to guide their decision on hiring a company to assist with meeting the regulations. We may provide further guidance on competencies for maritime security organizations, as necessary, but do not intend to list organizations, provide standards within the regulations, or certify organizations." We require security assessments to be protected from unauthorized disclosures and will enforce this requirement,