

vessel-to-vessel activities. A DoS is a document that establishes an agreement between a vessel and a facility, or between vessels, on their security arrangements to ensure their coordination and communication is clearly set out.

In the notice of meeting, we requested comments addressing recommendations for those operations or security levels when the DoS would be appropriate to facilitate coordination of security measures between a vessel and facility. As requested, we received comments addressing our question. Comments supported the intent of the requirements but expressed confusion at when it was needed. In particular, ferry operators questioned if they would be required to submit a DoS for every transit. Other commenters suggested that the DoS only be required at higher MARSEC Levels (2 and 3) for specific operations and are not appropriate for domestic vessels. Additionally, commenters suggested that transfers that are brief or involve barges should not have DoS requirements.

We believe a DoS is a valuable security communication tool for vessels, facilities and for COTPs. While a DoS is generally a MARSEC Levels 2 or 3 tool, there are certain operations that benefit from added coordination between the facility and the vessel. In the AMS requirements found elsewhere in today's **Federal Register**, each AMS Plan will be required to address DoS requirements for certain operations within the ports, especially related to MARSEC Levels 2 and 3. In addition, the AMS Plan will be required to include the procedures for what actions to take when vessels are at a higher MARSEC Level than the Port and request a DoS or other security measures in order to enter the Port. A DoS will not be required for all vessels and all facilities in all operations. In addition to the requirements found in the AMS Plan, both the Vessel Security and the Facility Security interim rules found elsewhere in today's **Federal Register** discuss when and for what operations a DoS will be required. We have determined that some operations always require a DoS and therefore vessels engaged in those operations may need to complete a DoS on a regular basis, due to their high-risk operations or locations. However, we believe a standing procedure or agreement can be used to meet this requirement. The COTP may determine, based on the localized repetitive nature of an operation, that a standing agreement which lays out the information in a DoS, can replace the daily use of the DoS.

We also requested comments in our public notice on how long a DoS should be kept on file (we suggested 2 years) and asked how the format of a DoS should be promulgated (guidance or regulation). In addition, the ISPS Code allows flag administrations to give guidance on when their ships should request a DoS during a port call or when interacting with other vessels. Many commenters suggested that a 2-year time frame for record retention was much too long. Many commenters also noted that they preferred guidance rather than regulation on the format for a DoS. Based on comments we received and to further align with the ISPS Code requirements, the Vessel Security requirements found elsewhere in today's **Federal Register** include requirements to keep DoS's on file for the vessel's last 10 port calls. The Facility Security requirements found elsewhere in today's **Federal Register** include requirements to keep DoS's on file for at least 90 days. As for DoS format, the interim rules mentioned above specify required elements for a DoS to ensure facility and vessel forms are acceptable for COTP reviews. For U.S. flag vessels, we intend to provide guidance to Company Security Officers on when to request a DoS based on vessel operations and world threat conditions.

7. *Security of Information Contained in Port, Vessel and Facility Security Assessments and Plans.* The ISPS Code, part A, sections 9 and 16, and the MTSA (46 U.S.C. section 70101(d)) require documents related to security, especially security assessments and plans, to be kept in a manner that is protected from unauthorized access or disclosure. In our notice of meeting, we asked for comments on whether a classification for sensitive security material would be useful in the implementation of National Maritime Security initiatives.

The majority of commenters supported a designation for all security-related materials to ensure this information is not available to the general public and some requested a higher security designation such as what the Defense Department is using. Some other commenters did not want a security-related designation because they wished to ensure the Freedom of Information Act remained primary to all information. Other commenters suggested that individuals should have clearances to see this material or that the Coast Guard be the only agency allowed to review the material. In contrast, some State and local government representatives stated their wish to have access to the material and

wanted us to include provisions for this access. Additionally, some commenters stated that a federal preemption clause was needed for this designation to ensure that if material was protected from disclosure at the federal level, a loophole at the State or regional level did not compromise its security.

Security-related information has traditionally not been in the public forum since it inherently puts at risk the very system that is being protected. Understanding the imperative need to safeguard maritime security material to ensure its dissemination does not make the vessel, facility, or port vulnerable to a transportation security incident, we have included provisions in this interim rule noting this type of material is to be designated as SSI in accordance with 49 CFR part 1520. Information designated as SSI is generally exempt under FOIA, and we believe that State disclosure laws that conflict with 49 CFR part 1520 are preempted by that regulation.

We did not believe that a security designation above SSI was needed for this material however, we did include provisions in this interim rule for a COTP to designate a higher level of security if there are provisions in the AMS Plan that indicate a higher level is appropriate. Access to the AMS Plan will be limited to those on the Area Maritime Security (AMS) Committee that have agreed to protect the material in a manner appropriate to its security sensitivity and have a need to know the material. Guidance on SSI and its use will be issued to assist AMS Committee members, consistent with 49 CFR part 1520. For material that is designated at a level higher than SSI, the COTP will screen AMS Committee members for appropriate clearances and take precautions appropriate to the material's sensitivity. Individuals and Federal agencies outside those with transportation oversight authority will not be allowed to view plans or assessments of vessels and facilities unless circumstances provide a need to view it. As stated in the Vessel Security interim rule found elsewhere in today's **Federal Register**, certain portions of each vessel security plan and assessment must be made accessible to authorities; however, those portions not required to be disclosed are protected with the SSI designation and need-to-know criteria. Owners and operators of vessels and facilities may also request a determination of a higher designation than SSI for their plans. The Commandant or the COTP, whoever is responsible for reviewing the security plan, will retain the designation authority. In all cases, the material, if retained by a Federal agency, must be