

communicating MARSEC Directives. One commenter said there should be one U.S. agency responsible for disseminating non-classified security information to shippers who do not have security clearances. Some commenters asked if vessel agents would be able to obtain copies of a MARSEC Directive on behalf of the vessel owner or operator. Most stated that the current process for communicating MARSEC Directives is cumbersome and suggested the best practice to inform foreign vessels entering waters under the jurisdiction of the U.S. would be to notify each at the time they file their 96-hour Notice of Arrival.

We recognize that the MARSEC Directive provision in § 101.405 establishes a challenging process for distributing directives to the regulated community. To ensure nationwide consistency, MARSEC Directives are issued at the Commandant level and, therefore, will allow each MSO to serve as a “1-stop shop” for MARSEC Directives. When owners, operators, or appointed agents of an owner or operator are notified of a MARSEC Directive, information will be included indicating those that have a “need to know.” To verify that an owner or operator has the “need to know” the content of a MARSEC Directive, MSOs have several tools available to them, including a database of vessels and facilities and their owner and operator information. In addition, an MSO can determine if a Company Security Officer, Vessel Security Officer, or Facility Security Officer has a “need to know” if an approved Vessel Security Plan or Facility Security Plan is presented to them. Once a person has provided enough information for the MSO to verify that person’s “need to know” and status as a regulated entity, the MSO will provide the MARSEC Directive. The “need to know” designation is required to protect sensitive security information from being exploited. We also recognize that further guidance should be provided to ensure communication expectations are clearly outlined and intend to update the guidance in NVIC 9-02 (Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports) to address distribution of MARSEC Directives.

One commenter asserted that there needs to be a means for industry and stakeholders to provide input or feedback both before and after the MARSEC Directive becomes effective, considering their knowledge of what will or will not work in an effective shipboard security program.

The regulations, in § 101.405, currently limit the authority to issue MARSEC Directives to the Commandant or his/her designee; however, we intend to consult other Federal agencies having an interest in the subject matter prior to issuing MARSEC Directives. When appropriate and as time permits, we intend to further consult with the affected industry. Section 101.405(d) also provides for an owner or operator to propose equivalent security measures in the event that they are unable to comply with MARSEC Directives.

Two commenters anticipated that MARSEC Directives would be prescriptive and that the Coast Guard should grant alternatives and equivalencies under these Directives. One commenter asked whether a recipient of a MARSEC Directive can maintain equivalent security measures for the duration of the directive, which could be open-ended, or if the recipient would have a certain amount of time to specifically comply with the MARSEC Directive.

We agree that there should be opportunities for owners and operators to implement alternatives or equivalent security measures to those prescribed in a MARSEC Directive. We provided these opportunities in § 101.405, which governs § 104.145 (MARSEC Directives), to allow equivalent security measures to be submitted to the Coast Guard in lieu of the specific measures required in a MARSEC Directive. Equivalencies approved by the Coast Guard under a specific MARSEC Directive will be in effect for the duration of that Directive.

Two commenters stated that our regulations suggest that information designated as sensitive security information is exempt from the Freedom of Information Act (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.

Three commenters stated that § 101.405(a)(2) refers to a “covered

person” as a term defined in 49 CFR 1520 related to sensitive security information. However, upon review of those regulations, they did not find a definition of “covered person” in those regulations.

We agree that the terminology in § 101.405(a)(2) is confusing. Therefore, we are clarifying § 101.405(a)(2) by amending the phrase “require owners or operators to prove that they have a ‘need to know’ the information in the MARSEC Directive and that they are a ‘covered person’” to read “require the owner or operator to prove that they are a person required by 49 CFR 1520.5(a) to restrict disclosure of and access to sensitive security information, and that under 49 CFR 1520.5(b), they have a need to know sensitive security information.”

One commenter suggested that we amend § 101.405 and change the words “may” and “should” to read “will” and “shall.”

We do not believe the recommended editorial changes add significant value or clarity.

We received three comments on Recognized Security Organizations (RSO). One commenter believed that any question of “underperformance” on the part of an RSO should be taken up with the flag state that has made the designation and should not, in the first instance, be sufficient justification for the application of control measures on a vessel that has been certified by the RSO in question. Another commenter recommended that the Coast Guard maximize national consistency and transparency with regard to the factors that are evaluated in the targeting matrix. One commenter supported the Coast Guard’s plan to use Port State Control to ensure that Vessel Security Assessments, Plans, and International Ship Security Certificates (ISSCs) approved by designated RSOs comply with the requirements of SOLAS and the ISPS Code.

In conducting Port State Control, the Coast Guard will consider the “underperformance” of an RSO. However, a vessel’s or foreign port facility’s history of compliance will also be important factors in determining what actions are deemed appropriate by the Coast Guard to ensure that maritime security is preserved.

Two commenters stated that in its control and compliance measures, the Coast Guard should clarify its legal authority to establish a security zone beyond its territorial sea.

One basis for the Coast Guard to establish security zones in the EEZ is pursuant to the Ports and Waterways Safety Act, 33 U.S.C. 1221 *et seq.* For