

Guard and IMO requirements. One commenter suggested that the Coast Guard include information to coordinate and provide access to regulatory compliance tools on a website. The commenter also suggested that the preamble accompanying the final rules should have well-named headings to assist the regulated community in locating information, including language explaining the applicability of SOLAS and including a list of contracting governments.

We intend to be flexible in the implementation of communication reporting methods to be used by vessel and facility owners or operators, and we are working on a website to provide security information to the regulated community. We encourage owners or operators to implement a system that best allows them to meet the reporting and recordkeeping requirements of their approved security plan. Additionally, the Coast Guard has provided headings throughout this preamble, based on the subparts of these security rules, to assist the public in locating information. SOLAS applicability is clearly defined in SOLAS and IMO maintains a list of contracting governments, which can be found on IMO's website (<http://www.imo.org>).

Twenty commenters made suggestions regarding reporting to the National Response Center (NRC) under § 101.305. Five commenters did not support notification to the NRC for all breaches of security. Two commenters stated that because the scope of the term "transportation security incident" and the meaning of the terms "may result" and "breach of security" are not clear, the regulated community is at risk of both over-reporting and under-reporting suspicious activity. Three commenters also suggested that the Coast Guard make a distinction between suspicious activities and an actual transportation security incident. Four commenters stated that it is not clear what the NRC would do with the information about suspicious incidents or how such a notification would sufficiently improve facility security in concert with other reporting processes for suspicious activity or security incidents. Eight commenters suggested that notifying the NRC "without delay" will not provide for the quickest response and suggested that owners or operators be allowed to: (1) Activate the security plan; (2) notify local law enforcement; (3) notify the local COTP; (4) use VHF channel 16 to notify the local area; or (5) notify the NRC "as soon as practical."

The Coast Guard provided a distinction between suspicious activities and a transportation security

incident in part 101. A "transportation security incident" is defined in § 101.105, as "a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area." As stated in § 101.305(a), a "suspicious activity" is an activity that may result in a transportation security incident. The purpose of requiring vessel and facility owners or operators to report suspicious activities or breaches of security "without delay" to the NRC is to enable the Coast Guard to identify patterns of this type of activity on a national scale and consult with other Federal agencies to confirm if the activity is a coordinated threat to our nation. The NRC will also relay to the COTP, and as appropriate port stakeholders, vessels, and facilities, reports of suspicious activities, breaches of security, and information concerning security-related patterns and trends. Because it is imperative to identify nationwide threat patterns, we did not amend the reporting requirements for suspicious activities or breaches of security. In the case of a transportation security incident, the notification goes, without delay, to the COTP or cognizant District Commander for OCS facilities, because of the need to assess impacts to the port area and to implement the AMS Plan, as appropriate.

Subpart D—Control Measures for Security

This subpart concerns control and compliance measures, including enforcement, MARSEC Directives, and penalties.

Seventeen commenters urged the Coast Guard to fully recognize the need for consistency in the application and enforcement of security-related regulations and in the plan approval process across several COTP zones.

We do recognize the need for consistency in the application and enforcement of the regulations. Therefore, the Coast Guard will continue to develop guidance for COTPs to consistently implement and enforce the security regulations.

Two commenters stated that the "entire issue of the authority to issue a MARSEC Directive" needed clarification. In addition, the commenters noted that in § 101.405(a)(1), the Commandant may delegate the authority to issue MARSEC Directives and indicated that this authority should remain with the Commandant.

MARSEC Directives are necessary as a mechanism to provide specific instruction to achieve the performance

standards required by these regulations and 46 U.S.C. Chapter 701 but that should not be open to the general public. As such, the MARSEC Directives will be labeled as sensitive security information because they will contain information that, if disclosed, could be used to exploit security systems and measures. MARSEC Directives will be issued under an extension of the Coast Guard's existing COTP authorities regarding maritime security, found in 33 U.S.C. 1226 and 50 U.S.C. 191. In part, the implementing regulations for 50 U.S.C. 191, found at 33 CFR 6.14–1 and promulgated by Executive Order 10277, contemplate action by the Commandant that is national in scope. Specifically, these regulations authorize the Commandant to prescribe such conditions and restrictions deemed necessary under existing circumstances for the security of certain facilities or public and commercial structures and vessels. Additionally, 43 U.S.C. 1333(d) authorizes the Coast Guard to establish certain requirements for OCS facilities. Moreover, MARSEC Directives are a necessary and integral part of carrying out the Coast Guard's authorities in 46 U.S.C. Chapter 701. The Commandant, at this time, intends to retain the authority to issue all MARSEC Directives.

Forty-three commenters requested clarification on issuance and receipt of MARSEC Directives. Several suggested that the Coast Guard: allow companies to submit a national "security sensitive information form," rather than notifying each COTP that companies have a "need to know" the security sensitive information contained in MARSEC Directives; have MSOs make Directives from all other MSOs available, which will allow them to have "1-stop shop" service; and, develop a secure website where individuals with sensitive security information authorization could access directives from all COTP zones. Many stated that owners and operators should not be required to comply with MARSEC Directives if they cannot or are not allowed to access the information in the Directive when that information is sensitive security information. Some were concerned that owners and operators would not know if they had a "need to know" the information in a MARSEC Directive under § 101.405(a)(2). Several comments asked for clarification of who will be granted access to applicable MARSEC Directives. One commenter requested a standardized process for applying for "need to know" status. One commenter argued that proof of a "need to know" undermines the purpose of