

and efficient manner. In contrast, many other commenters strongly opposed the extension of this system to the domestic fleet and questioned the functionality of it; asking what would be the resulting action once an alert was sent, especially from a remote location. Additionally, some commenters stated a desire to voluntarily install the equipment and use the system once it has been proven effective on a large scale.

While we believe an alert system is a valuable way to communicate to law enforcement if a vessel operator perceives a threat or a security incident is imminent, alternatives can also be used that may also prove effective (such as code words in a routine radio call or a pre-designated call word). Until vessel plans and AMS Plans are established and exercised to evaluate communications and identify gaps, we do not intend to extend this requirement to domestic vessels. However, if future communication exercises prove that alert systems already within the maritime community do not adequately address the appropriate vessels, we may require them in a separate rulemaking. Therefore, in the Vessel Security requirements found elsewhere in today's **Federal Register**, we have only applied the requirement to those vessels obligated to meet the SOLAS requirement.

36. *Fixed and Floating Platforms Requirements.* The International Maritime Organization issued a resolution titled, "Establishment of Appropriate Measures to Enhance the Security of Ships, Port Facilities, MODUs on Location and Fixed and Floating Platforms not covered by Chapter XI-2 of the 1974 SOLAS Convention" which was adopted by the Conference on Maritime Security as Resolution 7 on December 12, 2002. This resolution encourages Contracting Governments to consider security requirements for these maritime operators and platforms. In the notice, we discussed these international efforts and requested comments on whether security requirements should be placed on the offshore fixed and floating platforms.

Many comments were received which emphasized that fixed and floating platforms should be addressed within the port security plan. However, some commenters disagreed stating that even if included in a port security plan, the degree of security would be very different among platforms due to the potential for different enforcement procedures. Other commenters supported the position that while security measures are appropriate for MODUs and fixed and floating

platforms, but believed that any regulations should be carefully tailored to the unique operating environment of the offshore oil and natural gas exploration industry. These commenters also noted that, in their opinion, only a minimal amount of offshore platforms actually pose a viable security risk.

In accordance with the MTSA, we conducted an initial assessment on vessels and U.S. facilities as discussed in the *Applicability of National Maritime Security Initiatives* section above. Working with the Mineral Management Service (MMS) we identified certain operational quantities and personnel thresholds that are at a higher risk of a transportation security incident. Therefore, in the OCS Facility Security requirements found elsewhere in today's **Federal Register**, we have only applied requirements to those offshore platforms. However, we are also concerned about the consistency of security measures throughout the offshore community and have worked extensively with industry to develop standards that substantially improve security for this industry. The American Petroleum Institute (API) recommended practice titled, "API RP70 Security for Offshore Oil and Natural Gas Operations, 1st Edition" is available and its use is strongly encouraged for all owners and operators in this industry. Other platforms not included in the narrow operational category discussed above will be covered as part of the AMS Plan requirements in the "Area Maritime Security" (USCG-2003-14733) interim rule found elsewhere in today's **Federal Register**. However, in the future, we intend to review the need for further security requirements related to the offshore industry and may require compliance with industry standards such as API RP70 under a separate rulemaking.

37. *Seafarers' Identification Criteria Requirements.* In our notice of meeting, we noted the MTSA (46 U.S.C. 70111) requires the Secretary to establish enhanced crewmember identification. In addition, section 103 of the MTSA encourages the Secretary to negotiate an agreement for an international system of identification for seafarers. The Coast Guard has been working with other agencies of DHS (e.g., TSA and Immigration and Naturalization Service), the Department of State, the Maritime Administration, and others to support the work of the International Labour Organization (ILO). In the notice, we stated our intent to await the outcome of the June 2003 ILO conference prior to developing further seafarer identification domestic policy. Because this interim rule has been

published in a timeframe that did not allow us to incorporate the results of the ILO conference into it, we will issue any further requirements pertaining to seafarer identification under a separate rulemaking, if appropriate.

In addition to the above, the U.S. Government is mandated through the MTSA (46 U.S.C. 70105) to develop and implement a Transportation Security Card to control access to secure areas on a vessel or facility. Other agencies of DHS (e.g., TSA) have been developing the TWIC to satisfy the MTSA requirement. Pilot testing of the TWIC is scheduled for two ports, each in communication with a Transportation Security Administration central control point. This pilot project allows the other agencies of the DHS (e.g., TSA) to leverage key regional stakeholders and analyze life cycle and cost benefits, as well as the performance of various forms of identification technologies.

Recognizing that the implementation of the TWIC and the ILO efforts on seafarers identification involve substantial negotiation and development, we requested comments on our existing clarification of regulations notice titled "Maritime Identification Credentials" published in the **Federal Register** on April 7, 2002 (67 FR 51082). This document can be viewed on the DOT Document Management System at <http://dms.dot.gov> under Docket # USCG-2002-12917. We requested comments in the notice of whether changes to this clarification were needed or if other forms of identification should be recognized in the interim.

Many commenters suggested that we accept merchant mariner documents (MMD) and facility-issued ID cards as a form of identification. Some commenters stated that the existing requirements the Coast Guard set out in its clarification notice are sufficient until the TWIC project is complete. The majority of commenters submitted specific recommendations or suggestions with regard to the TWIC.

Under the current clarification notice, identification such as an MMD or a facility-issued card meeting the requirements set out in the notice are acceptable. Based on the lack of comments requesting amendments to the clarification, we will not amend the requirements at this time. We have incorporated them into this interim rule in order to ensure personal identification is addressed in subchapter H. We will also continue furthering the identification efforts at ILO and through the TWIC project. Comments received on this docket that relate to the TWIC project have been