

security-related issues and have discussed or required security measures on vessels and facilities (including offshore facilities) since well before the development of the ISPS Code or the MTSA. In this work, we have reviewed and assisted in the development of many industry standards for security that implement high security standards and are effective in preventing security-related incidents. In addition, we have worked with many States that have successfully developed crime prevention standards for the maritime community that are substantial and effective. Recognizing the substantial body of work in various maritime industry sectors on security, we anticipate recognized industry-developed standards to provide the backbone for implementing many of the security measures contained in the maritime security interim rules found in today's **Federal Register**. Key to this recognition will be a comprehensive review of the industry-developed standard to determine whether it is equivalent to the security requirements being met by those using the standards found in the maritime security interim rules in today's **Federal Register**. It is imperative that the industry-developed standards be deemed equivalent in order to ensure that those vessels and facilities that use the industry-developed standards and have a high likelihood of experiencing a transportation security incident have adequately reduced their risk to the benefit of the entire U.S. Marine Transportation System (MTS).

Commenters requested that the requirements be flexible enough to tailor measures to different industries and be performance based rather than prescriptive. Fundamental to the requirements for security has been the concept of a security assessment. This assessment is specifically linked to security plans and is focused on a vessel, facility, or port as a unique operation. Thus, the assessment results drive the security measures implemented to set or increase each security level and, thus, make each plan unique as well as performance-based. The enforcement of security measures is always difficult when dealing with a purely performance-based system, as opposed to a prescriptive one; however, in this case, it will be clear whether access control, for example, exists or does not. The requirements contained in the maritime security interim rules found in today's **Federal Register** include clear measures to conduct standard security assessments and draft standard security plans throughout the

maritime community. This approach will result in security plans which incorporate specific measures, unique to the operation, but in overall alignment with the objectives of all plans, to detect and deter a transportation security incident.

Commenters requested that the requirements be consistent among ports. We recognized the need for industry to have requirements tailored to their specific and diverse operations yet be afforded the consistency of the larger port-wide security measures. This said, no port has the same critical operations or geographic constraints, which make mandating the same security measures ineffective. However, we believe the framework of assessments and plans as laid out in the maritime security interim rules found in today's **Federal Register**, provides the consistency between ports and will be effective. This approach should ensure industry concerns are addressed within each COTP's area of responsibility. Each AMS Plan will also be reviewed and approved at both the District and Area level to assess consistency across the maritime community and to emphasize coordination across all borders. Additionally, we have included some flexibility in the AMS Plan requirements so that some geographic areas can be treated as systems, such as the Western Rivers, the Great Lakes, or the OCS. This geographic coordination of security measures to encompass an entire system will promote effective as well as efficient maritime security for all.

Commenters raised concern on the restrictions to mariner shore leave, detention aboard their vessels, and service provider access to mariners, such as port chaplains, union representatives, etc. This is a very important issue and it is addressed in the Vessel and Facility Security interim rules found elsewhere in today's **Federal Register**. The interim rules encourage both the vessel and the facility operators to coordinate shore leave for mariners, as well as procedures for access through the facility by visitors, including port chaplains and union representatives.

Commenters raised concern over the high cost of requirements and disparity between federal funds for the maritime versus the aviation sectors. We understand that many believe the cost of security is overwhelming. The requirements in this set of interim rules focus on those on those vessels and facilities that are at a higher risk of having a transportation security incident. We have developed flexible measures to meet the security

requirements. The disparity between funding available between transportation modes is outside the scope of this rulemaking. There are, however, programs, such as the Maritime Security Grant Program, which is funded through the Transportation Security Administration and jointly administered by the Maritime Administration, Coast Guard and the Transportation Security Administration. This grant program can provide some funding for owners and operators regulated under subchapter H. An excellent reference for this program can be found at <https://www.portsecuritygrants.dot.tsa.net>.

Commenters voiced a desire to have the Transportation Security Card requirements promulgated quickly. As discussed under issue number 37 in the *Specific Comments on the 40 issues listed in the public notice* section below, there are many credentialing efforts in development. 46 U.S.C. 70105, Transportation Security Cards, addresses unescorted personnel access to secure areas of facilities and vessels. Other agencies of DHS (e.g., TSA) are responsible for implementing this section of the MTSA. Other agencies of DHS (e.g., TSA) are developing the Transportation Worker Identification Credential (TWIC) that will be a transportation system-wide common credential, used across all modes, for all U.S. transportation workers requiring unescorted physical and logical access to secure areas of our transportation system. The goal is to have one standardized credential that is universally recognized and accepted across our transportation system and can be used locally within the current facility infrastructure. We recognize that personnel access control will be a component in vessel and facility security plans, and understanding that facilities and vessels will not want to create and install personnel access control systems in advance of the TWIC infrastructure. In order to address these competing concerns, guidelines will be developed jointly by other agencies of DHS (e.g., TSA) and the modal administrations, and will provide for acceptable personnel access control measures that can be used until the TWIC is available. These guidelines will address procedural measures.

Commenters requested that we provide guidelines on training requirements for vessel and facility security. The ISPS Code specifies the designation of a Company Security Officer, Ship Security Officer and a Port Facility Security Officer and details their required competencies, duties, and responsibilities. To supplement these