

involved in a transportation security incident. Further discussion on this risk and how we developed and assessed it for the maritime community is presented in the Applicability of National Maritime Security Initiatives discussion in this preamble.

In aligning the MTSA Section 102 requirements with the SOLAS amendments and the ISPS Code security requirements, we consider that the implementation of these requirements is best done through mandating compliance with the SOLAS amendments and the ISPS Code. The Coast Guard considers ISPS Code, part B, an essential element to ensure full and effective compliance with the intent of the MTSA. Foreign flag vessels entering the U.S. will be expected to carry valid International Ship Security Certificates (ISSC) and have the security plans fully implemented. The relevant provisions in ISPS Code, part B, will be taken into account by Port State Control Officers to assess if the security plan is fully implemented as required by the interim rules found elsewhere in today's **Federal Register**. The flag administration may also choose to provide a document or endorsement to the ISSC to verify that the security plan was based upon full compliance with the relevant provisions of ISPS Code, part B, to assist Coast Guard Port State Control Officers. We intend to implement strong Port State Control measures to aggressively enforce these regulations that will include tracking the performance of all owners, operators, flag administrations, recognized security organizations, charterers, and port facilities. Noncompliance will subject the vessel to a range of control and compliance measures, which could include denial of entry into port or significant delay. We will strictly enforce compliance with SOLAS and the ISPS Code for foreign SOLAS vessels, including assessing the risks posed by such vessels and any control measures that may be required when they call on foreign port facilities that do not comply with SOLAS and the ISPS Code, and we will similarly ensure that other vessels or port facilities covered by these regulations meet the requirements of this subchapter. A vessel's or port facility's history of compliance, or lack thereof, or security incidents involving a vessel or port facility, will be important factors in determining what actions are deemed appropriate by Coast Guard Port State Control Officers to ensure that maritime security is preserved. As mentioned, the performance of the owner, operator, flag

administration, recognized security organization, charterer, or port facility related to maritime security will also be some of the other factors that will be considered for the enforcement of maritime security in the U.S.

In addition to tracking performance, the Coast Guard's Port State Control program will also closely scrutinize an Administration's designation of recognized security organizations to ensure that those organizations fully meet the competencies and qualifications in the ISPS Code. Vessels with International Ship Security Certificates issued by recognized security organizations that are not properly designated, or that do not meet the required competencies and qualifications, will be subject to strict control measures, including possible expulsion from port and denial of entry into the United States. Therefore, it is imperative that Administrations carefully evaluate an organization through a rational process, adhering to the stringent criteria in the ISPS Code and any future standards that are developed by IMO, before designating the organization as a recognized security organization and delegating certain security functions to it.

The requirements for the AIS interim rule found elsewhere in today's **Federal Register** align with the recent amendments to SOLAS Chapter V, Regulation 19 that were adopted during the IMO Diplomatic Conference in December 2002 and the MTSA (specifically, MTSA sec. 102(e) and 46 U.S.C. 70114).

Impact on Existing Domestic Requirements

Many current requirements for security exist that are impacted by the interim rules published in today's **Federal Register**. 33 CFR part 120, Security of Vessels, and 33 CFR part 128, Security of Passenger Terminals, currently exist but apply only to certain cruise ships. We do not intend to revise 33 CFR parts 120 or 128 in the Vessel Security interim rule found elsewhere in today's **Federal Register**. However, in the future, this part may be revised or entirely deleted. This will consolidate the security requirements for all vessels in subchapter H. If this change to 33 CFR part 120 is made, foreign vessels that are required to comply with part 120 will be required to meet the requirements of part 104 including § 104.295 *Additional requirements—Cruise Ships* and passenger terminals that are required to comply with part 128 will be required to meet part 105.

The requirements in the interim rules also refer to and amend certain parts of

46 CFR and 49 CFR to ensure certificate of inspection requirements and other sections pertaining to facilities will include the new subchapter H requirements.

Notice of arrival requirements found in 33 CFR 160 have also been amended in the Vessel Security interim rule found elsewhere in today's **Federal Register** to ensure security-related information is provided to appropriate authorities prior to a vessel's entry into port. Additionally, the Captain of the Port (COTP) authorities within 33 CFR have been revised to ensure security-related elements and authorities are clearly highlighted.

Applicability of National Maritime Security Initiatives

As required in section 102 of the MTSA (46 U.S.C. section 70102a), the Coast Guard conducted an assessment of vessel types and U.S. facilities on or adjacent to the waters subject to the jurisdiction of the U.S. to identify those vessel types and U.S. facilities that pose a high risk of being involved in a transportation security incident. The MTSA defines a transportation security incident as a security incident resulting in a significant loss of life, environmental damage, a disruption to the transportation system, or economic disruption in a particular area.

Method of Assessment

In October 2001, the U.S. Coast Guard urgently needed to prioritize vessels and facilities based on the vulnerabilities to potential security threats and the consequences of potential incidents. We used a systematic, scenario-based process known as Risk-Based Decision Making (RBDM) to meet those needs. RBDM ensured a comprehensive evaluation by considering the relative risks of various target and attack mode combinations or scenarios. This provided a more realistic estimation of risk (and more efficient risk management activities) than a simple "worst-case outcome" assessment where only the worst possible consequences were considered.

In addition, the RBDM approach was based on the recommendations from the U.S. General Accounting Office (GAO). Managing risk is one of the best tools to complete a security assessment and to determine appropriate security measures (GAO-01-822). The GAO recommended a comprehensive security threat and risk assessment process (GAO-01-1158T).

Another GAO report, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, illustrated a scenario-based, risk