

Coast Guard published a series of final rules implementing portions of the maritime security initiatives mandated by MTSA, including the vulnerability assessment and security plan requirements. The USCG final rules provide a list of tools that may be used to conduct vulnerability self-assessments. This list includes TMSARM, a no-cost, web-based, flexible vulnerability assessment tool designed by TSA specifically to meet the requirements of MTSA.

**FOR FURTHER INFORMATION CONTACT:** For additional information or questions, contact Nick Lakis, Office of Maritime and Land Security, Transportation Security Administration Headquarters, West Building, Floor 9, TSA-8, 601 South 12th Street, Arlington, VA 22202-4220; e-mail: [nick.lakis@dhs.gov](mailto:nick.lakis@dhs.gov). For issues regarding the DHS/TSA's vulnerability self-assessment tool, contact Lynne Wolstenholme, Office of Threat Assessment and Risk Management, Transportation Security Administration Headquarters, West Tower, Floor 9, TSA-3, 601 South 12th Street, Arlington, VA 22202-4220; e-mail: [tsarisk@dhs.gov](mailto:tsarisk@dhs.gov).

#### **SUPPLEMENTARY INFORMATION:**

##### **Background**

On October 22, 2003, the USCG published in the **Federal Register** (68 FR 60447) a series of final rules, codified in the new Subchapter H of Title 33 of the Code of Federal Regulations (CFR), which adopted, with changes, the series of temporary interim rules published July 1, 2003 (68 FR 39240). This series of rules addresses security assessments and plans, as well as other security standards, measures, and provisions that are mandated by the Maritime Transportation Security Act (MTSA) of 2002 (Pub. L. 107-295, 116 Stat. 2064, Nov. 25, 2002). One of these MTSA requirements is that any facility or vessel that might be involved in a transportation security incident (TSI) conduct a vulnerability assessment and submit a security plan to the USCG by December 31, 2003. The MTSA defines a TSI as "a security incident that results in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area."

TSA, in coordination with other Federal agencies, academia, and industry, developed a vulnerability self-assessment tool, the TSA Maritime Self-Assessment Risk Module (TMSARM), specifically to meet the security assessment requirements mandated by MTSA. This TSA tool is briefly discussed in the preamble of the USCG

final rules. The tool supports three basic functions: (1) Capturing a current snapshot of the user's security system baseline; (2) providing users with a vulnerability assessment tool; and (3) assisting users in their development of a comprehensive security plan. TMSARM is available to Company Security Officers (CSO), Vessel Security Officers (VSO), and Facility Security Officers (FSO). This outstanding service is specific to TMSARM and is available to TMSARM users at no cost. The tool is easily accessible on TSA's website at [http://www.tsa.gov/public/interapp/editorial/editorial\\_0826.xml](http://www.tsa.gov/public/interapp/editorial/editorial_0826.xml), and the user determines all ratings. Any information entered into the tool will not become accessible to the Federal government unless and until the party entering the data formally submits this information to the TSA.

##### **Elements of the Self-Assessment Tool**

Although the USCG provides examples of security assessment tools in 33 CFR 101.510, the list is not intended to be exhaustive. The USCG does not require owners or operators to conduct security assessments using a specific tool, provided that the assessments meet the requirements of its regulations. TMSARM is merely one means of satisfying the USCG requirements.

In general, TMSARM focuses on preventing and mitigating a base array of threat scenarios developed for the various categories of vessels and facilities that comprise the maritime transportation sector and are covered by the USCG rules. Users rate their vessel/facility in terms of target attractiveness and several consequence categories that broadly describe health and well-being, economic consequence, and symbolic value. Users will first list the vessel/facility's baseline security countermeasures that apply for each of the threat scenarios and then rate the effectiveness of the countermeasures in detecting and preventing terrorist's actions against each of the provided threat scenarios. The countermeasures are divided into broad countermeasure groupings that represent different security layers that may be implemented against the various threat scenarios. Descriptive guidance for the effectiveness rating is provided for each of the countermeasure categories. The performance-based effectiveness ratings range from very high to very low, and describe the vessel/facility's ability to thwart the threat.

TSA has also developed guidance documents for the security countermeasure categories. These documents guide users on how to populate the sections of their security

plans with the security information developed through use of both the TMSARM security checklist and the TMSARM vulnerability assessment tool. Additionally, the guidance documents identify specific security vulnerabilities from the USCG regulations and map them to the appropriate TMSARM security countermeasure effectiveness descriptions within the tool. Once vulnerabilities are identified, very specific guidance on how to fill out form USCG Form CG-6025 (Vulnerability and Security Measures Summary) is provided.

After the tool is applied across each of the provided threat scenarios to determine baseline countermeasures, users can re-apply the tool to assess the impact of adding new countermeasures or enhancing existing countermeasures. Additional or enhanced countermeasures are included in the security plan along with estimated resource requirements and a timeframe for implementation. Upon completion, users receive a report that summarizes their inputs. This report can be included in the security plan that is required to be submitted to the USCG. Users' input to the tool becomes part of a vulnerability assessment, which constitutes Sensitive Security Information (SSI) under TSA regulations at 49 CFR part 1520. SSI may be released only to persons with a need to know, except with the written permission of the TSA Administrator. Unauthorized release of SSI may result in civil penalties or other action.

Issued in Arlington, Virginia, on December 1, 2003.

**James M. Loy,**  
*Administrator.*

[FR Doc. 03-30281 Filed 12-4-03; 8:45 am]

**BILLING CODE 4910-62-P**

#### **DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT**

**[Docket No. FR-4809-N-49]**

##### **Federal Property Suitable as Facilities To Assist the Homeless**

**AGENCY:** Office of the Assistant Secretary for Community Planning and Development, HUD.

**ACTION:** Notice.

**SUMMARY:** This Notice identifies unutilized, underutilized, excess, and surplus Federal property reviewed by HUD for suitability for possible use to assist the homeless.

**FOR FURTHER INFORMATION CONTACT:** Mark Johnston, room 7266, Department of Housing and Urban Development,