INFORMATION COLLECTION SUPPORTING STATEMENT

Department of Homeland Security–Vulnerability Identification Assessment Tools–Transportation (DHS VISAT-T

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information. (Annotate the CFR parts/sections affected).

In 2003, TSA determined that it was appropriate to develop a risk assessment tool to assist in decision making and to assist owners and operators of transportation assets to perform vulnerability assessments and develop security programs. GAO report 02-150T[1] identified that a good risk management program would include three basic functions: consequence, threat, and vulnerability. TSA took this approach to develop a software tool that would support this risk management approach and to make it available to the public, free of charge, through the Internet. The tool was first made available in 2003. The tool has provided useful information to TSA on security measures deployed and their effectiveness. TSA seeks to continue collecting this information and assist asset owners and operators.

On December 5, 2003 (68 FR 68096), TSA published in the Federal Register a Notice of Availability of TSA's maritime vulnerability self-assessment tool, the TSA Maritime Self-Assessment Risk Module (TMSARM), developed in coordination with other Federal agencies, academia, and industry, to support the U. S. Coast Guard's (USCG) regulatory efforts promulgated pursuant to the Maritime Transportation Security Act (MTSA) of 2002 (Pub. L. 107–295, Nov. 25, 2002, 116 Stat. 2064). MTSA regulations mandate that any facility or vessel that might be involved in a transportation security incident conduct a vulnerability assessment and submit a security plan to the USCG.

TSA developed the Department of Homeland Security–Vulnerability Identification Self-Assessment Tool–Transportation (DHS-VISAT-T), from the TSA Self-Assessment Risk Module (TSARM), as a means to gather security-related data in all modes of transportation. DHS-VISAT-T represents the U.S. Government's first self-assessment tool that provides the following features:

- The tool is provided to users at no cost;
- The tool is voluntary; and
- The tool is web-based and easily accessible.

TSA designed the self-assessment tool to be flexible to support the unique characteristics of each transportation mode, while still providing a common framework from which analysis and trends can be identified.

[1] "Homeland Security: Key Elements of a Risk Management Approach" (GAO-02-150T, October 12, 2001).

Department of Homeland Security–Vulnerability Identification Assessment Tools–Transportation (DHS VISAT-T

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.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

Stakeholders from every mode of transportation may request an account to access the assessment tool. The voluntary, self-assessment tool contains two sections. In the first section of the tool, users answer a series of questions, divided into seven countermeasure categories, to develop a comprehensive picture of the asset's security system posture. The countermeasure categories include:

- Plans, Policies, and Procedures;
- Security Training;
- Access Control;
- Physical Security Assets;
- Security Technologies and Equipment;
- Communications Security; and
- Information Security.

The second section of the tool focuses on the prevention and the mitigation of a base array of threat scenarios developed for different categories of assets. Users rate their asset in terms of target attractiveness (from a terrorist's perspective) and several consequence categories that describe health and well-being, economic consequences, and symbolic value of the asset. Users first list the asset's baseline security countermeasures that apply for each of the threat scenarios and then rate the effectiveness of the countermeasures in detecting and/or preventing the terrorist's actions against each threat scenario. Descriptive guidance for the effectiveness rating is provided for each of the countermeasure categories. The performance-based effectiveness ratings describe the asset's ability to thwart the threat.

After the tool is applied considering baseline countermeasures, users apply the tool two additional times to assess the impact of adding new countermeasures or enhancing existing countermeasures. The first additional assessment assumes a general increase in the national threat level (code orange). The second additional assessment assumes that the asset is known to be a specific target (code red). It is intended that the enhanced countermeasures will increase the security effectiveness compared to the baseline effectiveness ratings.

Upon completion of the tool, users receive a report that summarizes their inputs. This report can be used to develop a security plan. Results can also be used to identify areas of potential vulnerability. Users have the option to submit the completed assessment to TSA. If submitted, TSA reviews the assessment for consistency and provides feedback to the users.

Submitted assessments are then used to conduct analysis of the industry standard and to provide cross sector analysis of multiple modes.

The web-based tool asks a series of questions and then provides an output in the form of a vulnerability assessment. The tool takes approximately eight hours to complete (depending on internet connection and speed). The results collected are stored in a database for Government use to conduct vulnerability analysis to establish trends and weakness within each mode. Results of the data will help in establishing mitigating strategies to protect each mode of transportation.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden. [Effective 03/22/01, your response must SPECIFICALLY reference the Government Paperwork Elimination Act (GPEA), which addresses electronic filing and recordkeeping, and what you are doing to adhere to it. You must explain how you will provide a fully electronic reporting option by October 2003, or an explanation of why this is not practicable.]

TSA developed the web-based software to gather security related information from stakeholders and to assist stakeholders. The use of the web-based tool saves time and money for both the stakeholders and the Government. Current vulnerability assessments conducted by the private sector average one to two weeks in duration and cost thousands of dollars through the services of security professionals. The web-based tool is free to the stakeholder and takes approximately 8 hours to complete.

The process for stakeholders to acquire access to the tool is outlined below:

1. Stakeholder sends an email to the TSARisk help desk.[tsarisk@dhs.gov]

2. Help desk requests information to verify the user and the asset, and to tailor the customer account.

3. Help desk sends and email with the web address, username, and tool instructions.

4. Help desk sends a second email with the password and an attachment on Sensitive Security Information (SSI) protection.

5. Stakeholder logs into the secure web site, reads introductory screen, and selects “accept” button to continue.

Department of Homeland Security–Vulnerability Identification Assessment Tools–Transportation (DHS VISAT-T

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purpose(s) described in Item 2 above

This tool feeds into TSA's Risk Management Reporting System (RMRS). RMRS gathers data from different vulnerability assessment tools and gives the Office of Intelligence, Risk Support Division the ability to process and analyze the collected data to support national security. Currently, no other similar tool or electronic database is used to collect and analyze baseline security aspects in the transportation sector.

5. If the collection of information has a significant impact on a substantial number of small businesses or other small entities (Item 5 of the Paperwork Reduction Act submission form), describe the methods used to minimize burden.

TSA does not anticipate a significant impact on a substantial number of small businesses or other small entities. In an effort to reduce any resulting impact, TSA has designed DHS-VISAT-T with user-friendly features:

- The tool is provided to transportation asset owners/operators at no cost.
- The tool is voluntary.
- The tool is web-based and easily accessible.

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

If this collection were not offered to respondents, TSA would lose an opportunity to obtain important information to fulfill its statutory mission in transportation security.

7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with the general information collection guidelines in 5 CFR 1320.5(d)(2).

This collection will be conducted consistent with the guidelines set forth in 5 CFR 1320.5(d)(2).

8. Describe efforts to consult persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported. If applicable, provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d) soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.

TSA, in cooperation with other Federal, state, and local agencies, will coordinate with trade associations and industry partners in affected modes to establish business best practices for each new mode.

As required by 5 CFR 1320.8(d), TSA published in the Federal Register a notice for public comment on December 24, 2008 (73 FR 69670). To TSA's knowledge, no comments have been received in response to this notice.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

TSA does not provide any gift or payment to respondents.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

Information that users input to the tool becomes part of a vulnerability assessment that will be protected from disclosure, as Sensitive Security Information (SSI) under TSA regulations (49 CFR part 1520) and under the applicable Freedom of Information Act (FOIA) exemptions (particularly Exemption 3) of 5 U.S.C. 552(b). Because certain aspects of the VISAT constitute SSI under TSA regulations, users must not release vulnerability assessment information to persons who do not have a need to know, as defined in TSA's regulations at 49 CFR part 1520. By clicking the "agree" button on the web tool, the user acknowledges the applicability of SSI and accepts the obligation to handle the SSI in accordance with part 1520. This obligation applies to any printed version of the SSI that the user prints from an electronic version, and to any information that will become SSI upon submission to TSA.

Exemption 4 of the FOIA protects commercial or financial information submitted to the Government that is privileged or confidential. The exemption protects submitters who furnish commercial or financial information to the Government on a voluntary or a required basis by safeguarding them from the competitive disadvantages that could result from public disclosure of this information. If the information is voluntarily submitted, it is afforded protection as confidential information if it is not customarily released by the submitter to the public. A submission is voluntary if the Government does not require submission of particular information. The choice by an entity to participate in a Government activity does

not determine whether a submission is voluntary. Once the Government determines that the information is voluntarily provided and the submitter does not customarily release this information to the public, it is afforded protection from public release under Exemption 4 of the FOIA. Users therefore will be asked to acknowledge that information inputted to the tool is:

1. Considered proprietary commercial or financial commercial information by the user;

2. The user customarily limits distribution of this information within user's organization to those with a need-to-know;

3. The user customarily physically marks this information as proprietary and/or confidential, and;

4. The user customarily protects this information from release to the user's competitors and the general public.

11. Provide additional justification for any questions of sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.

Questions of sensitive nature are not incorporated in the tool or in the verification process for access to the tool.

12. Provide estimates of hour burden of the collection of information.

The tool functionality requires the user to navigate through a series of seven categories of checklist questions. The length of each question varies for each mode and for each category within the mode. Following the checklist questions, the user then navigates to the scenario portion of the tool, which again varies on the number of scenarios per category. In general, tool navigation can range from four to eight hours depending on the quantity of questions and scenarios tailored to the category. Additionally, the more detailed the user responses, the longer the duration. As a general average, eight hours is a normal gauge for completing the tool.

Based on this average, the following are the estimated annual user hours:

Maritime Facilities	250 x 8	= 2,000 hours
Maritime Vessels	250 x 8	= 2,000 hours
Passenger Stations	500 x 8	= 4,000 hours

The estimated number of total potential users is 1,000. The estimated annual burden hours is therefore 8,000 (1,000 x 8 hours = 8,000 annual hours).

INFORMATION COLLECTION SUPPORTING STATEMENT

Department of Homeland Security–Vulnerability Identification Assessment Tools–Transportation (DHS VISAT-T

13. Provide an estimate of the total annual cost burden to respondents or recordkeepers resulting from the collection of information.

There is no cost burden to respondents for this collection.

14. Provide estimates of annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, and other expenses that would not have been incurred without this collection of information.

Acquisition costs from FY03 to date is approximately $3.25 million, and since FY05 the program office has incurred no operations and maintenance. Projected Operation and maintenance costs for FY09 are estimated at $60,000. Life cycle costs for the entire program will be less than $20 million.

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB Form 83-I.

The RMRS program has evolved since its inception in 2003. The 2005 reported burden figures changed significantly due to previously reported estimates, to a more accurate user figure base. Since 2005, TSA's program offices have either continued or discontinued use of VISAT. Due to these program changes, the VISAT reported burden figure decreased from an estimated 300,000 to 1,000. TSA's VISAT is one of many tools available to industry and TSA has not seen the use that it initially estimated. Under MTSA, the maritime sector is required to resubmit vulnerability assessments and security plans to the USCG every five years.

The cost burden reported figure has decreased significantly since 2003. Since 2005, the program office has incurred limited operations and maintenance costs. The operations and maintenance cost was rolled up into another program support costs. As of 2009 the program office will be responsible for operations and maintenance costs which have been estimated at $60,000 for the first year.

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

Individual assessments will not be reproduced or published for public dissemination. Consolidated assessments will be analyzed and used in summary reports.

INFORMATION COLLECTION SUPPORTING STATEMENT

Department of Homeland Security–Vulnerability Identification Assessment Tools–Transportation (DHS VISAT-T

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

TSA will display the expiration date as required.

18. Explain each exception to the certification statement identified in Item 19, "Certification for Paperwork Reduction Act Submissions," of OMB Form 83-I.

The DHS-VISAT-T tool will comply with the certification statement identified in item 19.