

TABLE E-1.—OVERVIEW OF PRIVACY THREATS AND MITIGATION MEASURES

Type of threat	Description of threat	Type of measures to counter/mitigate threat
Unintentional threats from insiders <sup>15</sup> .	Unintentional threats include gaps in the privacy policy; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians ( <i>i.e.</i> , personnel of organizations with custody of the information). These threats can be physical ( <i>e.g.</i> , leaving documents in plain view) or electronic in nature. These threats can result in insiders being granted access to information for which they are not authorized or not consistent with their responsibility.	These threats are addressed by a privacy policy consistent with Fair Information Practices, laws, regulations, and OMB guidance; (b) defining appropriate functional and interface requirements; development, integrating, and configuring the system in accordance with these requirements and best security practices; and testing and validating the system against those requirements; and (c) providing clear operating instructions and training to users and system administrators.
Intentional threat from insiders.	Threat actions can be characterized as improper use of authorized capabilities ( <i>e.g.</i> , browsing, removing information from trash) and circumvention of controls to take unauthorized actions ( <i>e.g.</i> , removing data from a workstation that has been not been shut off)..	These threats are addressed by a combination of technical safeguards ( <i>e.g.</i> , access control, auditing, and anomaly detection) and administrative safeguards ( <i>e.g.</i> , procedures, training).
Intentional and unintentional threats from authorized external entities <sup>16</sup> .	Intentional: Threats can be characterized as improper use of authorized capabilities ( <i>e.g.</i> , misuse of information provided by (US-VISIT) and circumvention of controls to take unauthorized actions ( <i>e.g.</i> , unauthorized access to system).. Unintentional: Flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians.	These threats are addressed by technical safeguards (in particular, boundary controls such as firewalls) and administrative safeguards in the form of periodic privacy policy and practice compliance audits and routine use agreements and memoranda of understanding which require external entities (a) to conform with the rules of behavior and (b) to provide safeguards consistent with, or more stringent than, those of the system or program.
Intentional threats from external unauthorized entities.	Threats actions can be characterized by mechanism: physical attack ( <i>e.g.</i> , theft of equipment), electronic attack ( <i>e.g.</i> , hacking or other unauthorized access, interception of communications), and personnel attack ( <i>e.g.</i> , social engineering).	These threats are addressed by physical safeguards, boundary controls at external interfaces, technical safeguards ( <i>e.g.</i> , identification and authentication, encrypted communications), and clear operating instructions and training for users and systems administrators.

<sup>15</sup> Here, the term "insider" is intended to include individuals acting under the authority of the system owner or program manager. These include users, system administrators, maintenance personnel, and others authorized for physical access to system components.

<sup>16</sup> These include individuals and systems that are not under the authority of the system owner or program manager, but are authorized to receive information from, provide information to, or interface electronically with the system.

[FR Doc. 05-13371 Filed 7-5-05; 8:45 am]

BILLING CODE 4410-10-C

## DEPARTMENT OF HOMELAND SECURITY

### Coast Guard

[USCG-2005-21004]

#### Collection of Information Under Review by Office of Management and Budget (OMB): 1625-0060, 1625-0081, and 1625-0083

**AGENCY:** Coast Guard, DHS.

**ACTION:** Request for comments.

**SUMMARY:** In compliance with the Paperwork Reduction Act of 1995, this request for comments announces that the Coast Guard has forwarded three Information Collection Requests (ICRs)—(1) 1625-0060, Vapor Control Systems for Facilities and Tank Vessels; (2) 1625-0081, Alternate Compliance Program; and (3) 1625-0083, Operational Measures for Existing Tank Vessels Without Double Hulls—abstracted below, to the Office of Information and Regulatory Affairs (OIRA) of the Office of Management and

Budget (OMB) for review and comment. Our ICR describes the information we seek to collect from the public. Review and comment by OIRA ensures that we impose only paperwork burdens commensurate with our performance of duties.

**DATES:** Please submit comments on or before August 8, 2005.

**ADDRESSES:** To make sure that your comments and related material do not reach the docket (USCG-2005-21004) or OIRA more than once, please submit them by only one of the following means:

(1)(a) By mail to the Docket Management Facility, U.S. Department of Transportation (DOT), room PL-401, 400 Seventh Street, SW., Washington, DC 20590-0001. (b) By mail to OIRA, 725 17th St., NW., Washington, DC 20503, to the attention of the Desk Officer for the Coast Guard.

(2)(a) By delivery to room PL-401 at the address given in paragraph (1)(a) above, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is (202) 366-9329. (b) By delivery to OIRA, at the address given in paragraph (1)(b)

above, to the attention of the Desk Officer for the Coast Guard.

(3) By fax to (a) the Facility at (202) 493-2298 and (b) OIRA at (202) 395-6566, or e-mail to OIRA at [oira-docket@omb.eop.gov](mailto:oira-docket@omb.eop.gov) attention: Desk Officer for the Coast Guard.

(4)(a) Electronically through the Web site for the Docket Management System at <http://dms.dot.gov>. (b) OIRA does not have a Web site on which you can post your comments.

The Docket Management Facility maintains the public docket for this notice. Comments and material received from the public, as well as documents mentioned in this notice as being available in the docket, will become part of this docket and will be available for inspection or copying at room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street, SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet at <http://dms.dot.gov>.

Copies of the complete ICRs are available through this docket on the Internet at <http://dms.dot.gov>, and also from Commandant (CG-611), U.S. Coast Guard Headquarters, room 6106 (Attn: Ms. Barbara Davis), 2100 Second Street

SW., Washington, DC 20593-0001. The telephone number is (202) 267-2326.

**FOR FURTHER INFORMATION CONTACT:** Ms. Barbara Davis, Office of Information Management, telephone (202) 267-2326 or fax (202) 267-4814, for questions on these documents; or Ms. Andrea M. Jenkins, Program Manager, Docket Operations, (202) 366-0271, for questions on the docket.

**SUPPLEMENTARY INFORMATION:** The Coast Guard invites comments on the proposed collections of information to determine whether the collections are necessary for the proper performance of the functions of the Department. In particular, the Coast Guard would appreciate comments addressing: (1) The practical utility of the collections; (2) the accuracy of the estimated burden of the collections; (3) ways to enhance the quality, utility, and clarity of the information that is the subject of the collections; and (4) ways to minimize the burden of collections on respondents, including the use of automated collection techniques or other forms of information technology.

Comments to DMS or OIRA must contain the OMB Control Number of the Information Collection Reports (ICRs) addressed. Comments to DMS must contain the docket number of this request, (USCG 2005-21004). For your comments to OIRA to be considered, it is best if OIRA receives them on or before August 8, 2005.

**Public participation and request for comments:** We encourage you to respond to this request for comments by submitting comments and related materials. We will post all comments received, without change, to <http://dms.dot.gov>, and they will include any personal information you have provided. We have an agreement with DOT to use their Docket Management Facility. Please see the paragraph on DOT's "Privacy Act Policy" below.

**Submitting comments:** If you submit a comment, please include your name and address, identify the docket number for this request for comment (USCG-2005-21004), indicate the specific section of this document or the ICR to which each comment applies, and give the reason for each comment. You may submit your comments and material by electronic means, mail, fax, or delivery to the Docket Management Facility at the address under **ADDRESSES**, but please submit them by only one means. If you submit them by mail or delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the Facility,

please enclose a stamped, self-addressed postcard or envelope.

The Coast Guard and OIRA will consider all comments and material received during the comment period. We may change the documents supporting this collection of information or even the underlying requirements in view of them.

**Viewing comments and documents:**

To view comments, as well as documents mentioned in this notice as being available in the docket, go to <http://dms.dot.gov> at any time and conduct a simple search using the docket number. You may also visit the Docket Management Facility in room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street, SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

**Privacy Act:** Anyone can search the electronic form of all comments received in dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the Privacy Act Statement of DOT in the **Federal Register** published on April 11, 2000 (65 FR 19477), or you may visit <http://dms.dot.gov>.

**Previous Request for Comments**

This request provides a 30-day comment period required by OIRA. The Coast Guard has already published the 60-day notice required by 44 U.S.C. 3506(c)(2) (70 FR 21805, April 27, 2005). That notice elicited two comments. The first comment relates to information collection 1625-0083. The commenter states that the Coast Guard should not allow vessels carrying toxics, including oil, into the U.S. unless they have double hulls and suggests that we discontinue the information collection. In general, the comment is beyond the scope of this information collection. Summarily, information collection 1625-0083 requires the master, owner, or operator of a tank vessel to record and document information that is necessary for the safe operation of the vessel and to manage operational procedures, records, and licenses. The recordkeeping requirements in this collection ensure that pilots are adequately informed of the vessel's status, maneuvering capabilities, and under-keel clearance before beginning a transit. This collection aids the Coast Guard by allowing inspectors to determine if a vessel is in compliance with the requirements contained in 33 CFR part 157. The supporting statement in the docket contains details of this collection. Collection of Information

(COI) 1625-0083 is one of many collections related to environmental protection and maritime security. The second comment relates to 1625-0060, Vapor Control Systems for Facilities and Tank Vessels. The commenter raises two points:

- Alternative methods of inspection should be allowed, and;
- Our estimated hour burden is too low—commenter used an example of it taking 800 to 1200 man-hours per year for one large facility to comply with 33 CFR 156.170(g)(3) requirements.

In response to the first point, the Coast Guard notes that 33 CFR part 156 already has a provision for the Captain of the Port (COTP) to consider and approve alternatives in general. Section 156.107 of that part allows the COTP to consider and approve alternatives, procedures, methods, or equipment standards to be used by a vessel or facility operator in lieu of any requirements in this part if certain conditions are met.

In response to the second point, the comments are beyond the scope of this notice. The equipment tests and inspections in 33 CFR 156.170 are covered by a different collection of information: 1625-0095, Oil and Hazardous Materials Pollution Prevention and Safety Records, Equivalents/Alternatives and Exemptions (see 1990 final rule entitled "Marine Vapor Control Systems," 55 FR 25396, 25427, June 21, 1990). The 1625-0095 collection has been approved through March 2006.

**Information Collection Request**

1. **Title:** Vapor Control Systems for Facilities and Tank Vessels.

**OMB Control Number:** 1625-0060.

**Type of Request:** Extension.

**Affected Public:** Owners and operators of facilities and tank vessels, and certifying entities.

**Forms:** None.

**Abstract:** The information is needed to ensure compliance with U.S. regulations for the design of facility and tank vessel vapor control systems (VCS). The information is also needed to determine the qualifications of a certifying entity.

**Burden Estimates:** The estimated burden has increased from 1,073 hours to 1,145 hours a year.

2. **Title:** Alternate Compliance Program.

**OMB Control Number:** 1625-0081.

**Type of Request:** Extension.

**Affected Public:** Recognized classification societies.

**Forms:** CG-3752.

**Abstract:** This information is used by the Coast Guard to assess vessels

participating in the voluntary Alternate Compliance Program (ACP) before issuance of a Certificate of Inspection.

*Burden Estimates:* The estimated burden has increased from 150 hours to 164 hours a year.

3. *Title:* Operational Measures for Existing Tank Vessels Without Double Hulls.

*OMB Control Number:* 1625-0083.

*Type of Request:* Extension.

*Affected Public:* Owners, operators and masters of certain tank vessels.

*Forms:* None.

*Abstract:* The information is needed to ensure compliance with U.S. regulations regarding operational measures for certain tank vessels while operating in the U.S. waters.

*Burden Estimates:* The estimated burden has decreased from 18,006 hours to 6,807.

Dated: June 30, 2005.

**Nathaniel S. Heiner,**

*Acting, Assistant Commandant for Command, Control, Communications, Computers and Information Technology.*

[FR Doc. 05-13385 Filed 7-6-05; 8:45 am]

**BILLING CODE 4910-15-P**

## DEPARTMENT OF HOMELAND SECURITY

### U.S. Citizenship and Immigration Services

[CIS No. 2359-05]

RIN 1615-ZA27

#### Automatic Extension of Employment Authorization Documentation for Honduran and Nicaraguan TPS Beneficiaries

**AGENCY:** U.S. Citizenship and Immigration Services, DHS.

**ACTION:** Notice.

**SUMMARY:** On November 3, 2004, U.S. Citizenship and Immigration Services (USCIS) of the Department of Homeland Security (DHS) published two Notices in the **Federal Register** extending the designations of Honduras and Nicaragua for Temporary Protected Status (TPS) until July 5, 2006, and automatically extending employment authorization documents (EADs) for the beneficiaries of TPS for Honduras and Nicaragua for six months, from January 5, 2005 until July 5, 2005. Beneficiaries of TPS for Honduras and Nicaragua are required to re-register and obtain new EADs.

However, because of the large number of beneficiaries for TPS for Nicaragua and Honduras, USCIS will not be able to process and re-issue new EADs for all such beneficiaries by the July 5, 2005

expiration date. Accordingly, USCIS has decided to extend the validity of EADs issued to Honduran or Nicaraguan nationals (or aliens having no nationality who last habitually resided in Honduras or Nicaragua) under the extension of the TPS designations for an additional 90 days, from July 5, 2005 until October 5, 2005. This Notice announces that extension and also explains how TPS beneficiaries and their employers may determine which EADs are automatically extended.

**DATES:** The extension of EADs is effective July 5, 2005.

**FOR FURTHER INFORMATION CONTACT:** Colleen Cook, Residence and Status Services, Office of Programs and Regulations Development, U.S. Citizenship and Immigration Services, Department of Homeland Security, 111 Massachusetts Avenue, NW., 3rd Floor, Washington, DC 20529, telephone (202) 514-4754.

#### SUPPLEMENTARY INFORMATION:

#### Why Is USCIS Automatically Extending the Validity of EADs for Honduran and Nicaraguan TPS Beneficiaries?

Considering the large number of applications, it is likely that many re-registrants will receive their new EAD after the expiration date of their current EAD. In order to prevent a gap in employment authorization for qualified re-registrants, DHS is extending the validity of applicable EADs to October 5, 2005.

#### Who Is Eligible To Receive an Automatic Extension of His or Her EAD?

To receive an automatic extension of his or her EAD, an individual must be a national of Honduras or Nicaragua (or an alien having no nationality who last habitually resided in Honduras or Nicaragua) who has applied for and received an EAD under the TPS designation of Honduras or Nicaragua. This automatic extension is limited to EADs bearing an expiration date of January 5, 2005, that were issued on either Form I-766, Employment Authorization Document, or Form I-688B, Employment Authorization Card. The EAD must also be either (1) a Form I-766 bearing the notation "A-12" or "C-19" on the face of the card under "Category," or (2) a Form I-688B bearing the notation "274a.12(a)(12)" or "274a.12(c)(19)" on the face of the card under "Provision of Law."

#### Must Qualified Individuals Apply for the Automatic Extension of Their TPS-Related EADs?

No, qualified individuals do not have to apply for this automatic employment

authorization extension to October 5, 2005.

#### What Documents May a Qualified Individual Show to His or Her Employer as Proof of Employment Authorization and Identity When Completing Form I-9, Employment Eligibility Verification?

For completion of the Form I-9 at the time of hire or re-verification, qualified individuals who are receiving a three-month extension of their EADs by virtue of this **Federal Register** Notice may present to their employer a TPS-based EAD as proof of identity and employment authorization until October 5, 2005. To minimize confusion over this extension at the time of hire or re-verification, qualified individuals may also present to their employer a copy of this **Federal Register** Notice regarding the automatic extension of employment authorization documentation to October 5, 2005. In the alternative, any legally acceptable document or combination of documents listed in List A, List B, or List C of the Form I-9 may be presented as proof of identity and employment eligibility; it is the choice of the employee.

#### How May Employers Determine Whether an EAD Has Been Automatically Extended Through October 5, 2005 and Is Therefore Acceptable for Completion of the Form I-9?

For purposes of verifying identity and employment eligibility or re-verifying employment eligibility on the Form I-9 until October 5, 2005, employers of Honduran and Nicaraguan TPS beneficiaries whose EADs have been automatically extended by this Notice must accept such EAD if presented. An EAD that has been automatically extended by this notice to October 5, 2005 will actually contain an expiration date of January 5, 2005, and must be either (1) a Form I-766 bearing the notation "A-12" or "C-19" on the face of the card under "Category," or (2) a Form I-688B bearing the notation "274a.12(a)(12)" or "274a.12(c)(19)" on the face of the card under "Provision of Law." New EADs or extension stickers showing the October 5, 2005 expiration date will not be issued. Employers should not request proof of Honduran or Nicaraguan citizenship. Employers presented with an EAD that has been extended pursuant to this **Federal Register** Notice, if it appears to be genuine and appears to relate to the employee, should accept the EAD as a valid "List A" document and should not ask for additional Form I-9 documentation. This action by USCIS