

and passwords; compartmentalizing databases; auditing software; and encrypting data communications.

ATS also monitors source systems for changes to the source data. The system manager, in addition, has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. ATS information is secured in full compliance with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive information security program.

Access to the risk assessment results and related rules is restricted to a limited number of authorized government personnel who have gone through extensive training on the appropriate use of this information and CBP policies, including for security and privacy. These individuals are trained to review the risk assessments and background information to identify individuals who may likely pose a risk. To ensure that ATS is being accessed and used appropriately, audit logs are created and reviewed routinely by CBP's Office of Internal Affairs.

RETENTION AND DISPOSAL:

The information initially collected in ATS is used for entry screening purposes. Records in this system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration. ATS both collects information directly, and derives other information from various systems. To the extent information is collected from other systems, data is retained in accordance with the record retention requirements of those systems.

The retention period for data specifically maintained in ATS will not exceed forty years at which time it will be deleted from ATS. Up to forty years of data retention may be required to cover the potentially active lifespan of individuals associated with terrorism or other criminal activities. The touchstone for data retention, however, is its relevance and utility. Accordingly, CBP will regularly review the data maintained in ATS to ensure its continued relevance and usefulness. If no longer relevant and useful, CBP will delete the information. All risk assessments need to be maintained because the risk assessment for individuals who are deemed low risk will be relevant if their risk profile changes in the future, for example, if terrorist associations are identified.

Additionally, certain data collected directly by ATS may be subject to shorter retention limitations pursuant to separate arrangements. The adoption of shorter retention periods may not be publicly disclosed if DHS concludes that disclosure would affect operational security, for example by giving terrorism suspects the certainty that their past travel patterns would no longer be known to U.S. authorities.

SYSTEM MANAGER(S) AND ADDRESS:

Executive Director, National Targeting and Security, Office of Field Operations, U.S. Customs and Border Protection, Ronald Reagan Building and Director, Targeting and Analysis, Systems Program Office, Office of Information Technology, U.S. Customs and Border Protection.

NOTIFICATION PROCEDURE:

Generally, this system of records may not be accessed for purposes of determining if the system is a record pertaining to a particular individual. (See 5 U.S.C. 552a(e)(4)(G) and (f)(1)).

General inquiries regarding ATS may be directed to the Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 (phone: (202) 344-1850 and fax: (202) 344-2791).

RECORD ACCESS PROCEDURES:

Generally, this system of records may not be accessed under the Privacy Act for the purpose of inspection. The majority of this system is exempted from this requirement pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

General inquiries regarding ATS may be directed to the Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW., Washington, DC 20229.

Requests should conform to the requirements of 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

CONTESTING RECORD PROCEDURES:

Since this system of records may not be accessed, generally, for purposes of determining if the system contains a record pertaining to a particular individual and those records, if any,

cannot be inspected, the system may not be accessed under the Privacy Act for the purpose of contesting the content of the record.

RECORD SOURCE CATEGORIES:

The system contains information derived from other law enforcement systems operated by DHS and other government agencies, which collected the underlying data from individuals and public entities directly.

In addition, the system contains information collected from carriers that operate vessels, vehicles, aircraft, and/or trains that enter or exit the United States.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to 31 CFR 1.36 pertaining to the Treasury Enforcement Communications System, the Automated Targeting System, which was previously covered by the Treasury Enforcement Communications System (TECS) system of records notice and associated with the below exemptions, records and information in this system are exempt from 5 U.S.C. 552a(c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). DHS intends to review these exemptions and, if warranted, issue a new set of exemptions specific to ATS within ninety (90) days of the publication of this notice.

Dated: October 27, 2006.

Hugo Teufel III,
Chief Privacy Officer.

[FR Doc. 06-9026 Filed 10-30-06; 3:31 pm]

BILLING CODE 4410-10-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[USCG-2005-22732]

Domestic Vessel Passenger Weights—Voluntary Interim Measures

AGENCY: Coast Guard, DHS.

ACTION: Notice; request for public comments.

SUMMARY: The Coast Guard announces supplemental guidance for owners and operators of small passenger vessels to avoid operation in environmental conditions that are inappropriate for their vessels. The Coast Guard is requesting public comments on this notice.

DATES: Comments and related material must reach the Docket Management Facility not later than January 31, 2007.

ADDRESSES: You may submit comments identified by Coast Guard docket number USCG–2005–22732 to the Docket Management Facility at the U.S. Department of Transportation. To avoid duplication, please use only one of the following methods:

(1) *Web site:* <http://dms.dot.gov>.

(2) *Mail:* Docket Management Facility, U.S. Department of Transportation, 400 Seventh Street, SW., Washington, DC 20590–0001.

(3) *Fax:* 202–493–2251.

(4) *Delivery:* 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. The telephone number is 202–366–9329.

FOR FURTHER INFORMATION CONTACT: If you have questions on this notice, call Mr. William Peters, Naval Architecture Division, G–PSE–2, Coast Guard, telephone 202–372–1372. If you have questions on viewing or submitting material to the docket, call Ms. Renee V. Wright, Program Manager, Docket Operations, telephone 202–493–0402.

SUPPLEMENTARY INFORMATION:

Request for Comments

All comments received will be posted, without change, to <http://dms.dot.gov> and will include any personal information you have provided. We have an agreement with the Department of Transportation (DOT) to use the Docket Management Facility. Please see DOT's "Privacy Act" paragraph below.

Submitting comments: If you submit a comment, please include your name and address, identify the docket number for this notice (USCG–2005–22732) and give the reason for each comment. You may submit your comments by electronic means, mail, fax, or delivery to the Docket Management Facility at the address under **ADDRESSES**; but please submit your comments 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. We will consider all comments received during the comment period.

Viewing comments and documents: To view comments, go to <http://dms.dot.gov> at any time, click on "Simple Search," enter the last five digits of the docket number for this rulemaking, and click on "Search." 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 into any of our 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 Department of Transportation's Privacy Act Statement in the **Federal Register** published on April 11, 2000 (65 FR 19477), or you may visit <http://dms.dot.gov>.

Background and Purpose

On April 26, 2006, the Coast Guard published a notice (71 FR 24732) that announced voluntary interim measures for certain domestic vessels to account for increased passenger and vessel weight when determining the number of passengers permitted. The notice included a discussion on the typical restriction to "reasonable operating conditions" placed on the Certificate of Inspection (COI) of vessels that are designed only for operation on protected waters. Under the recommended voluntary measures for prudent operation for all small passenger vessels, the notice advised that reasonable operating conditions do not include conditions associated with a small craft advisory as well as other specific wind and wave conditions.

According to the National Weather Service (NWS), a small craft advisory is issued to alert small craft—generally vessels less than 65 feet in length—to sustained (more than 2 hours) hazardous weather or sea conditions that may be either present or forecasted. Upon learning of such an advisory, the NWS urges mariners to immediately determine the reason and to monitor the latest marine broadcast. See <http://www.weather.gov/glossary>.

The April notice also discussed increased passenger weight and identified the means by which the Coast Guard typically evaluates a small passenger vessel's stability.

This notice updates the voluntary measures for prudent operation published in the **Federal Register** on April 26, 2006, by clarifying guidance in the previous notice on reasonable operating conditions and the vessels to which that guidance applies.

The Coast Guard received numerous comments from the public in response to the April 26, 2006, notice.

Advisory Actions

Updated Voluntary Measures for Prudent Operation: All Small Passenger Vessels

The recommendation given in the April 26, 2006, notice to owners and operators of all small passenger vessels certificated only for operation on protected waters is amended as follows to further clarify "reasonable operating conditions":

(1) For passenger pontoon vessels, voluntarily operate in "reasonable operating conditions," which do not include:

- Wind gusts over 30 knots (35 miles per hour);
- Waves over two feet;
- Sustained winds over 18 knots (21 miles per hour); or
- Conditions associated with a small craft advisory.

(2) For other small passenger, non-sailing vessels certificated to operate only on protected waters and that are less than 65 feet, give special consideration to the "reasonable operating conditions" as set forth in item (1) above while complying with the requirements of 46 CFR 185.304 or 122.304.

The Coast Guard expects that small passenger vessel owners and operators are aware of and follow the guidelines presented in the April 26, 2006 notice as supplemented by this notice. The Coast Guard is in the process of more formally addressing stability issues caused by increases in passenger and vessel weight for all domestic vessels.

Dated: October 25, 2006.

C.E. Bone,

Rear Admiral, U.S. Coast Guard, Assistant Commandant for Prevention.

[FR Doc. E6–18334 Filed 11–1–06; 8:45 am]

BILLING CODE 4910–15–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent To Request Renewal From OMB of One Current Public Collection of Information: Aircraft Operator Security

AGENCY: Transportation Security Administration, DHS.

ACTION: Notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on one currently approved information collection requirement abstracted below that we will submit to the Office of Management and Budget (OMB) for renewal in compliance with the Paperwork Reduction Act.