Dated: June 29, 2011.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011–16804 Filed 7–5–11; 8:45 am]

BILLING CODE 9110–9L–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2011–0061]

Privacy Act of 1974; Department of Homeland Security/ALL–030 Use of the Terrorist Screening Database System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 the Department of Homeland Security proposes to establish a new Department-wide system of records notice entitled, ''Department of Homeland Security/ALL–030 Use of the Terrorist Screening Database System of Records.'' The Department of Homeland Security is maintaining a mirror copy of the Department of Justice/Federal Bureau of Investigation–019 Terrorist Screening Records System of Records, August 22, 2007, in order to automate and simplify the current method for transmitting the Terrorist Screening Database to the Department of Homeland Security and its components. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register**. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before August 5, 2011. This new system will be effective August 5, 2011.

ADDRESSES: You may submit comments, identified by docket number DHS–2011–0061 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.
- *Docket:* For access to the docket to read background documents or comments received go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) proposes to establish a new system of records titled, ''DHS/ALL–030 Use of the Terrorist Screening Database (TSDB) System of Records.'' DHS is maintaining a mirror copy of the Department of Justice (DOJ)/Federal Bureau of Investigation (FBI)–019 Terrorist Screening Records System of Records (August 22, 2007, 72 FR 47073) in order to automate and simplify the current method for transmitting the TSDB to DHS and its components.

Homeland Security Presidential Directive 6 (HSPD–6), issued in September 2003, called for the establishment and use of a single consolidated watchlist to improve the identification, screening, and tracking of known or suspected terrorists and their supporters. The FBI/TSC maintains and distributes the TSDB as the U.S. government's consolidated terrorist watchlist. DHS and the FBI/TSC, working together, have developed the DHS Watchlist Service (WLS) in order to automate and simplify the current method for transmitting TSDB records from the FBI/TSC to DHS and its components.

The WLS allows the FBI/TSC and DHS to move away from a manual and cumbersome process of data transmission and management to an automated and centralized process. The WLS will replace multiple data feeds from the FBI/TSC to DHS and its components, as documented by information sharing agreements, with a single feed from the FBI/TSC to DHS and its components. The WLS is a system to system secure connection with no direct user interface.

DHS and its components are authorized to access TSDB records via the WLS pursuant to the terms of information sharing agreements with FBI/TSC. DHS is publishing this SORN and has published privacy impact assessments to provide additional transparency into how DHS has implemented WLS. DHS will review and update this SORN no less then biennially as new DHS systems come online with the WLS and are approved consistent with the terms of agreements with FBI/TSC. There are five DHS systems that currently receive TSDB data directly from the FBI/TSC and will use the WLS. These systems have existing SORNs that cover the use of the TSDB:

(1) Transportation Security Administration (TSA), Office of Transportation Threat Assessment and Credentialing: DHS/TSA–002 Transportation Security Threat Assessment System (May 19, 2010, 75 FR 28046);

(2) TSA, Secure Flight Program: DHS/TSA–019 Secure Flight Records System (November 9, 2007, 72 FR 63711);

(3) U.S. Customs and Border Protection (CBP), Passenger Systems Program Office for inclusion in TECS: DHS/CBP–011 TECS System (December 19, 2008 73 FR 77778);

(4) U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT) Program for inclusion into the DHS Enterprise Biometrics Service (IDENT): DHS/USVISIT–0012 DHS Automated Biometric Identification System (June 5, 2007, 72 FR 31080); and

In addition, two DHS components will receive TSDB data via the WLS in the form of a computer readable extract. The components' use of the TSDB data is covered by existing SORNs:

(1) Office of Intelligence and Analysis (I&A): DHS/IA–001 Enterprise Records System, (May 15, 2008 73 FR 28128), and

(2) U.S. Immigration and Customs Enforcement (ICE): DHS/ICE–009 External Investigations, (January 5, 2010 75 FR 404).

Information stored in the WLS will be shared back with the FBI/TSC in order to ensure that DHS and the FBI/TSC can reconcile any differences in the database and ensure DHS has the most up-to-date and accurate version of TSDB records. All other sharing will be conducted pursuant to the programmatic system of records notices and privacy impact assessments discussed in this SORN.

DHS is planning future enhancements to the WLS that will provide for a central mechanism to receive information from DHS components when they encounter a potential match to the TSDB and send this information to the FBI/TSC. DHS will update this SORN to reflect such enhancements to the WLS, as part of its biennial reviews of this SORN once that capability is implemented.

DHS is publishing this SORN to cover the Department's use of the TSDB in

order to provide greater transparency to the process.

Concurrent with the publication of this SORN, DHS is issuing a Notice of Proposed Rulemaking to exempt this system from specific sections of the Privacy Act.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/ALL–030 Use of the Terrorist Screening Database system of records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records DHS/ALL–030

SYSTEM NAME:

Department of Homeland Security (DHS)/ALL–030 Use of the Terrorist Screening Database (TSDB) System of Records

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained at DHS and Component Headquarters in Washington, DC and field offices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include:

- Individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (''known or suspected terrorists'').

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Identifying information, such as name, date of birth, place of birth, biometrics, photographs, passport and/or drivers license information, and other available identifying particulars used to compare the identity of an individual being screened with a known or suspected terrorist, including audit records containing this information;
- For known or suspected terrorists, in addition to the categories of records listed above, references to and/or information from other government law enforcement and intelligence databases, or other relevant databases that may contain terrorism information.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

- Homeland Security Act of 2002, Public Law 107–296;
- Section 5 U.S.C. 301;
- The Tariff Act of 1930, as amended;
- The Immigration and Nationality Act; and
- 49 U.S.C. 114, 5103a, 40113, ch. 49 and 46105.

PURPOSE(S):

DHS and its components collect, use, maintain, and disseminate information in the DHS Watchlist Service (WLS) to facilitate DHS counterterrorism, law enforcement, border security, and inspection activities. TSDB data, which includes personally identifiable information (PII), is necessary for DHS to effectively and efficiently assess the risk and/or threat posed by a person for the conduct of its mission.

The Federal Bureau of Investigation (FBI)/Terrorist Screening Center (TSC) is providing a near real time, synchronized version of the TSDB in order to improve the timeliness and governance of watchlist data exchanged between the FBI/TSC and DHS and its component systems that currently use watchlist data.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ)/FBI/TSC in order to receive confirmations that the information has been appropriately transferred and any other information related to the reconciliation process so that DHS is able to maintain a mirror copy of the TSDB.

This system will share information internal to the Department pursuant to (b)(1) of the Privacy Act. Besides the routine use described above, external sharing shall occur at the programmatic level pursuant to following published System of Records Notices:

(1) TSA, Office of Transportation Threat Assessment and Credentialing: DHS/TSA–002 Transportation Security Threat Assessment System (May 19, 2010, 75 FR 28046);

(2) TSA, Secure Flight Program: DHS/TSA–019 Secure Flight Records System (November 9, 2007, 72 FR 63711);

(3) CBP, Passenger Systems Program Office for inclusion in TECS: DHS/CBP–011 TECS System (December 19, 2008 73 FR 77778);

(4) U.S. VISIT program for inclusion into the DHS Enterprise Biometrics Service (IDENT): DHS/USVISIT–0012 DHS Automated Biometric Identification System (June 5, 2007, 72 FR 31080);

(5) Office of Intelligence and Analysis (I&A): DHS/IA–001 Enterprise Records System, (May 15, 2008 73 FR 28128), and

(6) U.S. Immigration and Customs Enforcement (ICE): DHS/ICE–009 External Investigations, (January 5, 2010 75 FR 404).

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Records may be retrieved by name or personal identifier.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

The WLS will maintain a near real time mirror of the TSDB, and will not retain historical copies of the TSDB. The WLS will be synchronized with the TSDB. When the FBI/TSC adds, modifies, or deletes data from the TSDB, the WLS will duplicate these functions almost simultaneously, and that information will then be passed to DHS and its component systems. The DHS component that is screening individuals will maintain, separate from the WLS, a record of a match or possible match with the TSDB and DHS will retain this information in accordance with the DHS component specific SORNs identified in this notice.

SYSTEM MANAGER AND ADDRESS:

Executive Director, Passenger Systems Program Office, Office of Information Technology, Customs and Border Protection, 7400 Fullerton Rd, Springfield, VA.

NOTIFICATION PROCEDURE:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS and its components will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP–0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury, as a substitute for notarization. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

In addition, if individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Inquiry Redress Program (TRIP) (January 18, 2007, 72 FR 2294). Individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through TRIP.

TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs such as airports and train stations or crossing U.S. borders. Redress requests should be sent to: DHS Traveler Redress Inquiry Program, 601 South 12th Street, TSA–901, Arlington, VA 20598 or online at *http://www.dhs.gov/trip* and at *http://www.dhs.gov*.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Records are received from the DOJ/FBI–019 Terrorist Screening Records System of Records (August 22, 2007, 72 FR 47073)

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12); (f); (g)(1); and (h) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(1) and (k)(2).

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011–16807 Filed 7–5–11; 8:45 am]

BILLING CODE P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2011–0539]

National Offshore Safety Advisory Committee; Vacancies

AGENCY: Coast Guard, DHS.

ACTION: Request for applications.

SUMMARY: The Coast Guard seeks applications for membership on the National Offshore Safety Advisory Committee. This Committee advises the Secretary of Department of Homeland Security on matters and actions concerning activities directly involved with or in support of the exploration of offshore mineral and energy resources insofar as they relate to matters within Coast Guard jurisdiction.

DATES: Applicants should submit a cover letter and resume in time to reach the Alternate Designated Federal Officer (ADFO) on or before August 22, 2011.

ADDRESSES: Applicants should send their cover letter and resume to the following address: Commandant (CG–5222), Attn: Vessel and Facility Operations Standards, U.S. Coast Guard, 2100 Second Street, SW., STOP 7126, Washington, DC 20593–7126; or by calling (202) 372–1386; or by faxing (202) 372–1926; or by e-mailing to *Kevin.Y.Pekarek2@uscg.mil.*