

below or sign up at the registration desk on the day of the meeting. The names and affiliations, if any, of individuals who address the Committee are included in the public record of the meeting. Please note that the public comment period may end before the time indicated, following the last call for comments. Written comments and requests to have a copy of your materials distributed to each member of the Committee prior to the meeting should be sent to Martha K. Landesberg, Executive Director, DHS Data Privacy and Integrity Advisory Committee, by September 30, 2011. Persons who wish to submit comments and who are not able to attend or speak at the meeting may submit comments at any time. All submissions must include the Docket Number (DHS-2011-0076) and may be submitted by any one of the following methods:

- *Federal eRulemaking Portal*: <http://www.regulations.gov>. Follow the instructions for submitting comments.

- *E-mail*: PrivacyCommittee@dhs.gov. Include the Docket Number (DHS-2011-0076) in the subject line of the message.

- *Fax*: (703) 483-2999.

- *Mail*: Martha K. Landesberg, Executive Director, Data Privacy and Integrity Advisory Committee, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions must include the words "Department of Homeland Security Data Privacy and Integrity Advisory Committee" and the Docket Number (DHS-2011-0076). Comments received will be posted without alteration at <http://www.regulations.gov>, including any personal information provided.

If you wish to attend the meeting, please plan to arrive at the Navy League Building by 12:45 p.m. The DHS Privacy Office encourages you to register for the meeting in advance by contacting Martha K. Landesberg, Executive Director, DHS Data Privacy and Integrity Advisory Committee, at PrivacyCommittee@dhs.gov. Advance registration is voluntary. The Privacy Act Statement below explains how DHS uses the registration information you may provide and how you may access or correct information retained by DHS, if any.

Docket: For access to the docket to read background documents or comments received by the DHS Data Privacy and Integrity Advisory Committee, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT:
Martha K. Landesberg, Executive

Director, DHS Data Privacy and Integrity Advisory Committee, Department of Homeland Security, Washington, DC 20528, by telephone (703) 235-0780, by fax (703) 235-0442, or by e-mail to PrivacyCommittee@dhs.gov.

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act (FACA), 5 U.S.C. App. 2 The DHS Data Privacy and Integrity Advisory Committee provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within the DHS that relate to personally identifiable information, as well as data integrity and other privacy-related matters. The committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. 451.

Agenda

During the meeting, the Chief Privacy Officer will provide the Committee an update on the activities of the DHS Privacy Office. The Committee will also receive updates on DHS FOIA operations by the Deputy Chief FOIA Officer and on Advanced Imaging Technology by the Transportation Security Administration's Privacy Officer. In addition, the Subcommittees will report on their work in support of the Committee's planned guidance on privacy protections for information sharing within DHS. The agenda will be posted in advance of the meeting on the Committee's Web site at <http://www.dhs.gov/privacy>. Please note that the meeting may end early if all business is completed.

Privacy Act Statement: DHS's Use of Your Information

Authority: DHS requests that you voluntarily submit this information under its following authorities: the Federal Records Act, 44 U.S.C. 3101; the FACA, 5 U.S.C. App. 2; and the Privacy Act of 1974, 5 U.S.C. 552a.

Principal Purposes: When you register to attend a DHS Data Privacy and Integrity Advisory Committee meeting, DHS collects your name, contact information, and the organization you represent, if any. We use this information to contact you for purposes related to the meeting, such as to confirm your registration, to advise you of any changes in the meeting, or to assure that we have sufficient materials to distribute to all attendees. We may also use the information you provide for public record purposes such as posting publicly available transcripts and meeting minutes.

Routine Uses and Sharing: In general, DHS will not use the information you provide for any purpose other than the Principal Purposes, and will not share this information within or outside the agency. In certain circumstances, DHS may share this information on a case-by-case basis as required by law or as necessary for a specific purpose, as described in the DHS/ALL-002 Mailing and Other Lists System of Records Notice (November 25, 2008, 73 FR 71659).

Effects of Not Providing Information: You may choose not to provide the requested information or to provide only some of the information DHS requests. If you choose not to provide some or all of the requested information, DHS may not be able to contact you for purposes related to the meeting.

Accessing and Correcting Information: If you are unable to access or correct this information by using the method that you originally used to submit it, you may direct your request in writing to the DHS Deputy Chief FOIA Officer at foia@dhs.gov. Additional instructions are available at <http://www.dhs.gov/foia> and in the DHS/ALL-002 Mailing and Other Lists System of Records referenced above.

Dated: September 9, 2011.

Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011-24223 Filed 9-20-11; 8:45 am]

BILLING CODE 9110-9L-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2011-0071]

Privacy Act of 1974; Department of Homeland Security, U.S. Citizenship and Immigration Services—004 Systematic Alien Verification for Entitlements Program System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of revision and republication of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to revise an existing Department of Homeland Security system of records notice titled "DHS/USCIS-004 Verification Information System" system of records and republish it as "DHS/USCIS-004 Systematic Alien Verification for Entitlements Program" system of records. Previously, the Department of

Homeland Security published a single system of records notice for both the E-Verify and Systematic Alien Verification for Entitlements Programs as part of the underlying technology, the Verification Information System on December 11, 2008. On May 11, 2010 the Department of Homeland Security published the Department of Homeland Security/ United States Citizenship and Immigration Services—011 E-Verify Program system of records. The Department of Homeland Security now proposes to revise and republish the Department of Homeland Security/ United States Citizenship and Immigration Services—004 Verification Information System system of records as the Department of Homeland Security/ United States Citizenship and Immigration Services—004 Systematic Alien Verification for Entitlements Program system of records. The United States Citizenship and Immigration Services Verification Division administers the Systematic Alien Verification for Entitlements Program. The Systematic Alien Verification for Entitlements Program is a fee-based intergovernmental initiative designed to help Federal, state, tribal, and local government agencies check immigration status when granting benefits, licenses, and other lawful purposes. On the publication of this SORN, the Verification Information System system of records notice will no longer be applicable. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before October 21, 2011. This new system will be effective October 21, 2011.

ADDRESSES: You may submit comments, identified by docket number DHS–2011–0071 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 Department of Homeland Security as 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 by the submitter.
- *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 please contact: Janice Jackson, Acting Privacy Branch, Chief, Verification Division, U.S. Citizenship and Immigration Services, Department of Homeland Security, 131 M Street NE., Suite 200, MS 2600, Washington, DC 20529. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

Congress mandated that the Immigration and Naturalization Service, as a precursor to the Department of Homeland Security (DHS) United States Citizenship and Immigration Services (USCIS), establish a system to verify the immigration status of individuals seeking government benefits. Authority for having a system for verification of citizenship and immigration status of individuals seeking government benefits can be found in the Immigration Reform and Control Act of 1986 (IRCA), Public Law (Pub. L.) 99–603; the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), Public Law 104–193, 110 Stat. 2168; Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104–208, 110 Stat. 3009; and the Real ID Act of 2005, Public Law 109–13. Based on these authorities and in accordance with the Privacy Act of 1974, 5 U.S.C. 552a, DHS USCIS proposes to establish a new DHS system of records titled “DHS/USCIS–004 Systematic Alien Verification for Entitlements Program System of Records.”

USCIS Verification Division administers the Systematic Alien Verification for Entitlements (SAVE) Program, a fee-based intergovernmental initiative designed to help Federal, state, tribal, and local government agencies check immigration status when granting benefits, licenses, and other lawful purposes. SAVE is supported by and uses information derived from individuals, partner agencies, the Verification Information System (VIS) and other DHS, Department of State, and Department of Justice systems.

The REAL ID Act of 2005, Public Law 109–13, 119 Stat. 231, 302 (2005) (codified at 49 U.S.C. 30301 note) requires all state Departments of Motor Vehicles (DMV) to utilize the USCIS SAVE program to verify the legal immigration status of applicants for

driver's licenses, driver's permits, and state-issued identification cards. Congress delayed the initial implementation date from May 2008 until December 2009. DMVs access SAVE through the American Association of Motor Vehicle Administrators Network (AAMVAnet) or via Internet access using Web 3 or Web Services, which is a support service that allows SAVE customer agencies to access VIS information through a software interface.

Previously, USCIS documented the SAVE and E-Verify Programs in the VIS Privacy Impact Assessment (PIA) and System of Records Notice (SORN). VIS was and continues to be the underlying technology of both systems. In order to assist the public in better understanding the two programs, USCIS has issued a separate E-Verify SORN and, with this publication, is updating the original VIS SORN with this updated SORN. SAVE is described in previous SORNs, most recently in the VIS SORN (73 FR 75445, December 11, 2008).

SAVE Usage Overview

The SAVE Program was originally limited to immigration status verification for eligibility determinations of any public benefit, license, or credential—the benefit or “entitlement” referred to in the name of the program. However, over time the scope of SAVE has grown to include the implementation of Section 642(c) of IIRIRA, which obligates USCIS to respond to inquiries “by a federal, state, or local government agency seeking to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law.” This expansion was highlighted in previous versions of the SAVE Privacy Impact Assessment (PIA).

Accordingly, to the extent that a Federal, state, or local government entity has the legal authority to verify immigration status, SAVE, as an access method to USCIS systems, is authorized to respond to the request. Specifically, in addition to verifications for purposes of granting government benefits, this includes verification for purposes of background investigations for individuals, and cohabitants of the individuals undergoing background investigations.

Government agencies input biographic information into SAVE for status determinations. If SAVE has a record pertaining to the individual, the government agency automatically receives limited biographic information on the citizenship and immigration status of the individual. If SAVE does

not have a record pertaining to the individual, SAVE prompts the customer agency asking if they would like a manual second step verification, with possible escalation to a manual third step verification, Form G-845, if appropriate. Although SAVE may receive a Social Security Number (SSN) from its supporting VIS systems or customer agencies as part of a status determination, it does not specifically request or return SSNs in its responses.

The primary use of the SAVE information is to provide immigration status information for any legally mandated purpose to Federal, state, and local government customer agencies. The majority of customer agencies use SAVE to determine if applicants are entitled to receive the public benefits, licenses, or credentials that they administer. For example, based on IRCA, customer agencies use SAVE when providing benefits such as education and housing assistance, unemployment benefits, and Medicaid or other state health insurance benefits. PRWORA, through its definition of public benefits, allows customer agencies to use SAVE to determine the immigration status for purposes such as granting licensing and loans. (IIRIRA) provides for customer agencies to use SAVE for any legal purpose, such as credentials, background investigations, and voter registration. In addition, the Real ID Act of 2005 requires that all states utilize SAVE to verify the immigration status of individuals claiming to be non-U.S. citizens for driver's licenses, driver's permits, and identification cards.

Information in SAVE will only be used for SAVE verifications and other purposes incidental to the SAVE process, such as customer agency registration and relationship management, user accountability, program quality management, and monitoring and compliance activities.

In accordance with the Privacy Act of 1974, DHS proposes to establish a new DHS system of records notice titled "DHS/USCIS-004—Systematic Alien Verification for Entitlements Program" system of records. The USCIS Verification Division administers the SAVE Program. SAVE is an intergovernmental initiative designed to assist benefit-granting Federal, state, and local agencies determine if non-U.S. citizen applicants are entitled to receive the public benefits, licenses, or credentials that they administer. Previously, DHS published a single system of records notice for the E-Verify and SAVE Programs as part of the underlying technology, VIS (73 FR 75445, December 11, 2008). DHS is now

publishing separate system of records notices for E-Verify and SAVE in order to assist the public in better understanding these programs. This newly established system of records will be included in DHS's inventory of record systems.

With the publication of this SAVE SORN to accompany the E-Verify SORN (76 FR 26738, May 9, 2011), the VIS SORN will be retired.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the U.S. 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 U.S. 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. Below is the description of the DHS/USCIS-004 Systematic Alien Verification for Entitlements Program 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/USCIS-004

SYSTEM NAME:

Department of Homeland Security U.S. Citizenship and Immigration Services—004 Systematic Alien Verification for Entitlements Program System of Records.

SECURITY CLASSIFICATION:

Unclassified, for official use only.

SYSTEM LOCATION:

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include both U.S. citizens and non-U.S. citizens covered by provisions of the Immigration and

Nationality Act of the United States, including individuals who have been lawfully admitted to the United States, individuals who have been granted or derived U.S. citizenship, and individuals who have applied for other immigration benefits pursuant to 8 United States Code (U.S.C.) 1103 *et seq.*

SAVE users are covered by the DHS/ALL-004—General Information Technology Access Account Records System SORN (74 FR 49882, last published September 29, 2009).

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Information collected from the benefit applicant by the customer agency to facilitate immigration status verification may include the following about the benefit applicant: receipt number, Alien Number (A-Number), admission number (I-94 number), name (last, first, middle), date of birth, country of birth, customer agency case number, DHS document type, DHS document expiration date, Immigration and Custom Enforcement's (ICE) Student and Exchange Visitor Identification System (SEVIS) ID, foreign passport number, visa number, social security number (in very limited circumstances using the Form G-845, Document Verification Request), and type of benefit(s) for which the applicant has applied (*e.g.*, unemployment insurance, educational assistance, driver licensing, *etc.*).

B. System-generated responses as a result of the SAVE verification process including case verification number and SAVE response.

C. Any information on the individual may be verified through SAVE from the following Federal databases: Arrival/Departure Information System (ADIS), Central Index System (CIS), Computer-Linked Application Information Management System 3 & 4 (CLAIMS 3 & CLAIMS 4), Customer Profile Management System (CPMS), Student and Exchange Visitor Identification System (SEVIS), Customs and Border Protection's (CBP) Nonimmigrant Information System and Border Crossing Information (NIIS and BCI), Enforcement Integrated Database (EID), Enforcement Alien Removal Module (EARM), Enterprise Document Management System (EDMS), Marriage Fraud Amendment System (MFAS), Microfilm Digitization Application System (MiDAS), National File Tracking System (NFTS), Refugees, Asylum, and Parole System (RAPS), Reengineered Naturalization Applications Casework System (RNACS), Image Storage and Retrieval System (ISRS), and immigration status (*e.g.*, Lawful Permanent Resident) from the

Department of Justice Executive Office of Immigration Review (EOIR) System (EOIR) and the Department of State the Consular Consolidated Database (DOS-CCD).

The individual information that may be verified through SAVE includes: A-Number, name (last, first, middle), date of birth, date entered into the United States (entry date), country of birth, class of admission code, file control office code, SSN, I-94 number, provision of law code cited for employment authorization, alien's status change date, date admitted until, country of citizenship, port of entry, departure date, visa number, passport number, passport information, passport card number, document receipt number, form numbers (e.g., Form I-551 Lawful Permanent Resident Card or Form I-766 Employment Authorization Document), SEVIS Identification Number (SEVIS ID), naturalization date, Federal Bureau of Investigation Number (FIN), beneficiary alien number, beneficiary date of birth, beneficiary country of birth, beneficiary SSN, beneficiary last name, beneficiary first name, beneficiary middle name, petitioner alien number, petitioner SSN, petitioner naturalization certificate number, petitioner first name, petitioner last name, petitioner firm name, and petitioner tax number. This information may also include spouse's name (last first, middle), date of birth, country of birth, country of citizenship, class of admission, date of admission, A-Number, receipt number, phone number, marriage date and place, and naturalization date and place; child's name(s) (last, first, middle), date of birth, country of birth, class of admission, A-Number; and employer information: Name, address, supervisor's name, and supervisor's phone number, case history, alerts, case summary comments, case category, date of encounter, encounter information, custody actions and decisions, case actions and decisions, bonds, and photograph, asylum applicant receipt date, airline and flight number, country of residence, city where boarded, city where visa was issued, date visa issued, address while in the United States, nationality, decision memoranda, investigatory reports and materials compiled for the purpose of enforcing immigration laws, exhibits, transcripts, and other case-related papers concerning aliens, alleged aliens, or lawful permanent residents brought into the administrative adjudication process.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for having a system for verification of immigration status is

found in IRCA, Public Law 99-603, 100 Stat. 3359; PRWORA, Public Law 104-193, 110 Stat. 2105; Title IV, Subtitle A, of IIRIRA, Public Law 104-208, 110 Stat. 3009; and the REAL ID Act of 2005, Public Law 109-13, 119 Stat. 231.

PURPOSE(S):

The purpose of the SAVE Program is to provide a fee-based intergovernmental service, which assists Federal, state, Tribal, or local government agencies, or contractors acting on the agency's behalf and licensing bureaus confirm immigration status information, to the extent that such disclosure is necessary to enable these agencies to make decisions related to: (1) Determining of eligibility for a Federal, state, or local public benefit; (2) issuing a license or grant; (3) issuing a government credential; (4) conducting a background investigation; or (5) any other lawful purpose.

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), including U.S. Attorney Offices, or other Federal agencies conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee of DHS in his/her official capacity;
3. Any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or
4. The U.S. or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individual that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, state, Tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To approved Federal, state, and local government agencies for any legally mandated purpose in accordance with their authorizing statute or law and where an approved Memorandum of Agreement (MOA) or Computer Matching Agreement (CMA) is in place between DHS and the entity.

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 of applicant or other unique identifier to include: Verification number, A-Number, I-94 number, SSN, Passport number, Visa number, SEVIS ID, or by the submitting agency name.

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 retention and disposal schedule, N1-566-08-7, has been approved by the National Archives and Records Administration. Records collected in the process of enrolling in SAVE and in verifying citizenship or immigration status are stored and retained in SAVE for ten (10) years from the date of the completion of verification, unless the records are part of an on-going investigation in which case they be retained until completion of the investigation. This period is based on the statute of limitations for most types of misuse or fraud possibly using SAVE (under 18 U.S.C. 3291, the statute of limitations for false statements or misuse regarding passports, citizenship, or naturalization documents).

SYSTEM MANAGER AND ADDRESS:

Chief, Verification Division, U.S. Citizenship and Immigration Services, 131 M Street NE., Suite 200, MS 2600, Washington, DC 20529.

NOTIFICATION PROCEDURE:

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 USCIS's 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., 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. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov> or 1-866-431-0486. 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.

RECORD ACCESS PROCEDURES:

See "Notification procedure" above.

CONTESTING RECORD PROCEDURES:

See "Notification procedure" above.

RECORD SOURCE CATEGORIES:

Records are obtained from several sources to include: (A) Agencies seeking to determine immigration status; (B) individuals seeking public licenses, benefits, or credentials; (C) information collected from the Federal databases listed in the Category of Records section above; and (D) information created by SAVE.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: August 26, 2011.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011-24221 Filed 9-20-11; 8:45 am]

BILLING CODE 9111-97-P

DEPARTMENT OF HOMELAND SECURITY**Coast Guard**

[USCG-2011-0869]

Information Collection Requests to Office of Management and Budget

AGENCY: Coast Guard, DHS.

ACTION: Sixty-day notice requesting comments.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995, the U.S. Coast Guard intends to submit Information Collection Requests (ICRs) to the Office of Management and Budget (OMB), Office of Information and Regulatory Affairs (OIRA), requesting approval of revisions to the following collections of information: 1625-0067, Claims under the Oil Pollution Act of 1990; and 1625-0068, State Access to the Oil Spill Liability Trust Fund for Removal costs under the Oil Pollution Act of 1990. Our ICRs describe the information we seek to collect from the public. Before submitting these ICRs to OIRA, the Coast Guard is inviting comments as described below.

DATES: Comments must reach the Coast Guard on or before November 21, 2011.

ADDRESSES: You may submit comments identified by Coast Guard docket number [USCG-2011-0869] to the Docket Management Facility (DMF) at the U.S. Department of Transportation (DOT). To avoid duplicate submissions, please use only one of the following means:

(1) *Online:* <http://www.regulations.gov>.

(2) *Mail:* DMF (M-30), DOT, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue, SE., Washington, DC 20590-0001.

(3) *Hand delivery:* Same as mail address above, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

(4) *Fax:* 202-493-2251. To ensure your comments are received in a timely manner, mark the fax, to attention Desk Officer for the Coast Guard.