Freedom of Information Act Officer, *http://www.dhs.gov* or 1–866–431–0486. In addition you should:

• Explain 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; and

• Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

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 the above 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 below: 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)

• 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 Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)

• 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)

• Student and Exchange Visitor Identification System (SEVIS)

• Immigration status (e.g., Lawful Permanent Resident) from the Department of Justice Executive Office of Immigration Review (EOIR), System and the Department of State the Consular Consolidated Database (DOS–CCD).

(D) Information created by the Systematic Alien Verification for Entitlements (SAVE) program.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: July 27, 2012.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2012–19207 Filed 8–7–12; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2012–0048]

Privacy Act of 1974; Department of Homeland Security U.S. Citizenship and Immigration Services –011 E-Verify Program System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled ''Department of Homeland Security/United States Citizenship and Immigration Services—011 E-Verify Program System of Records.'' The United States Citizenship and Immigration Services E-Verify Program allows employers to check citizenship status and verify employment eligibility of newly hired employees. The Department of Homeland Security is updating this Privacy Act System of Records Notice for the E-Verify Program in order to provide notice that E-Verify is: (1) Updating the ''Category of Individuals'' to remove USCIS employees and contractors, which are covered under the DHS/ALL–004 General Information Technology Access Account Records System SORN, and to remove individuals who have locked their Social Security Number (SSN) in E-Verify since this functionality is not available; (2) adding the collection of the foreign passport country of issuance (COI) from the employers using the recently updated Form I–9 and from the United States Visitor and Immigrant Status Indicator Technology (US–VISIT) Arrival and Departure Information System (ADIS) to the ''Categories of Records;'' (3) moving the list of sources of records from ''Category of Records'' to ''Record Source Categories,'' removing two decommissioned systems and adding two new systems to ''Record Source Categories;'' (4) removing the monitoring and compliance ''Category of Records'' because those are now covered by the Compliance Tracking and Management System (CTMS) SORN (74 FR 24022); (5) updating the system location information for the Verification Information System (VIS), the underlying technology supporting the E-Verify program, from a contractor-owned facility in Meriden, CT to a government-owned facility in Stennis, MS; (6) incorporating minor changes to the ''Routine Uses'' to improve clarity; and (7) adding COI to ''Retrievability'' as a way in which DHS may retrieve records in this system of records.

This updated system is included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before September 7, 2012. This updated system will be effective September 7, 2012.

ADDRESSES: You may submit comments, identified by docket number DHS–2012–0048 by one of the following methods:

• *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

• *Fax:* 202–343–4010.

• *Mail:* Jonathan R. Cantor, Acting 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 please contact: Brian C. Hobbs, (202–443–0114), Privacy Branch Chief, U.S. Citizenship and Immigration Services, Department of Homeland Security, 131 M Street NE., Suite 200 Mail Stop 2600, Washington, DC 20529. For privacy issues please contact: Jonathan R. Cantor (202–343–1717), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue the Department of Homeland Security system of records titled, ''Department of Homeland Security/U.S. Citizenship and Immigrations—011 E-Verify Program System of Records.'' The USCIS E-Verify Program allows employers to check citizenship status and verify employment eligibility of newly hired employees.

DHS is updating this Privacy Act System of Records Notice for the E-Verify Program in order to provide notice that E-Verify is: (1) Updating the ''Category of Individuals'' to remove USCIS employees and contractors, which are covered under the DHS/ALL–004 General Information Technology Access Account Records System SORN, and to remove individuals who have locked their SSN in E-Verify since this functionality is not currently available; (2) adding the collection of the foreign passport country of issuance (COI) from the employers using the recently updated I–9 Form and from the United States Visitor and Immigrant Status Indicator Technology (US–VISIT) Arrival and Departure Information System (ADIS) to the ''Categories of Records;'' (3) moving the list of sources of records from ''Category of Records'' to ''Record Source Categories,'' removing two decommissioned systems and adding two new systems to ''Record Source Categories;'' (4) removing the monitoring and compliance ''Category of Records'' because those are now covered by the Compliance Tracking and Management System (CTMS) SORN (74 FR 24022); (5) updating the system location information for the Verification Information System (VIS), the underlying technology supporting the E-Verify program, from a contractor-owned facility in Meriden, CT to a government-owned facility in Stennis, MS; (6) incorporating minor changes to the ''Routine Uses'' to improve clarity; and (7) adding COI to ''Retrievability'' as a way in which DHS may retrieve records in this system of records.

DHS is updating the ''Category of Individuals'' to remove USCIS employees and contractors. These individuals are covered under the DHS/ALL–004 General Information Technology Access Account Records System SORN. Additionally DHS is updating the ''Category of Individuals'' to remove individuals who have locked their SSN in E-Verify. Functionality that enables individuals to lock their SSNs is not available in E-Verify.

As described in more detail in the DHS/USCIS/PIA–030(d), E-Verify currently uses the I–94 number, which is generally issued to aliens at the time they lawfully enter the United States, as a primary identifier to determine employment eligibility for non-immigrants. U.S. Customs and Border Protection (CBP) is in the process of automating the I–94 system to increase efficiency and streamline the admission process for travelers to the United States. However, since E-Verify depends on the integrity of the I–94 number and the CBP's automation efforts are still underway, USCIS is updating it process for E-Verify by using a foreign passport number and COI as a primary identifier. A stand-alone passport number does not result in a unique primary identifier because multiple countries could issue the same passport number. Employers will enter the foreign passport number and COI. E-Verify will verify this data against ADIS.

In order to provide greater clarity in this SORN, USCIS has removed the sources of records that were described in the ''Category of Records'' and moved them to ''Source Record Categories.'' In addition to moving the list of source records, DHS has removed two sources, ISRS and RNACS, and added one new source of records, Customer Profile Management System (CPMS) for biometric information on individuals issued a Permanent Resident Card (Form I–551).

DHS removed the monitoring and compliance ''Category of Records'' because those are now covered by the Compliance Tracking and Management System (CTMS) SORN (74 FR 24022).

DHS is also providing public notice of the relocation of the VIS system. In alignment with OMB's Federal Data Center Consolidation Initiative, the DHS Office of the Chief Information Officer is consolidating 43 of the Department's legacy data centers into two Enterprise Data Centers (EDCs), known as Data Center (DC) 1 and DC2. The consolidation of numerous Component systems at our EDCs enables more effective collection and use of business information across the enterprise. VIS was originally stored in a contractor owned facility in Meriden, CT. Since the publication of the original SORN, the system has moved to the DHS-owned facility, DC1.

DHS is updating the routine uses to add additional clarity concerning the uses of data. These updates do not create any new sharing uses of data. The routine uses are being updated to add general language ensuring that ''[a]ny disclosure of information must be made consistent with the official duties of the person making the disclosure.'' Routine uses A, B, and D are being reworded to provide greater clarity and make non-substantive grammatical changes. Routine use C is being updated to change ''other federal government agencies'' to ''General Services Administration'' to better reflect the statutory authorities and the fact that records will be shared with the National Archives and Records Administration (NARA) where NARA maintains the records as permanent records.

DHS is updating ''Retreivability'' to include COI as a way in which DHS may retrieve records in this system of records.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the federal government agencies collect, maintain, use, and disseminate 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, the Department of Homeland Security 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/U.S. Citizenship and Immigration Services—011, E-Verify 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

Department of Homeland Security (DHS)/U.S. Citizenship and Immigration Services (USCIS)—011

SYSTEM NAME:

DHS/U.S. Citizenship and Immigration Services—011—E-Verify Program

SECURITY CLASSIFICATION:

Unclassified, for official use only.

SYSTEM LOCATION:

Records are maintained at the U.S. Citizenship and Immigration Services

(USCIS) Headquarters in Washington, DC and field offices; and at the DHS Stennis Data Center (DC1).

CATEGORIES OF UNDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by the E-Verify program include: employees, both U.S. Citizens and non–U.S. Citizens, whose employers have submitted to E-Verify their identification information; employers who enroll in E-Verify; designated agents who enroll in E-Verify; individuals employed or retained by employers or designated agents who have accounts to use E-Verify; individuals who contact E-Verify with information on the use of E-Verify; and individuals who provide their names and contact information to E-Verify for notification or contact purposes.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Information about the employee to be verified:

- Name (last, first, middle initial, maiden)
- Date of Birth
- Social Security Number
- Date of Hire
- Information related to the expiration of the three day hire
- Awaiting SSN
  - Technical Problems
  - Audit Revealed New Hire Was Not Run
  - Federal Contractor With E-Verify Clause Verifying Existing Employees
  - Other
- Claimed Citizenship Status
- Acceptable Form I–9 document type
- Expiration Date of Acceptable Form I–9 Document
- State or jurisdiction of issuance of identity document when that document is a driver's license, driver's permit, or state-issued identification (ID) card
- Passport Number and Country of Issuance
- Driver's license number, driver's permit number, or state-issued ID number if issued by a state or jurisdiction participating in the Records and Information from Departments of Motor Vehicles for E-Verify (RIDE) program and where an Memorandum of Agreement (MOA) exists between the state or jurisdiction and DHS USCIS to verify the information about the document
- Receipt Number
- Visa Number
- A-Number
- I–94 Number
- Employment Authorization Document (Form I–766) Number
- Permanent Residence Card (Form I–551) Number Photographs, if required by secondary verification

B. Disposition data from the employer. The following codes are entered by the employer based on what the employer does as a result of the employment verification information:

- The employee continues to work for the employer after receiving and Employment Authorized result: Employer selects this option based on receiving an Employment Authorized response from E-Verify;
- The employee continues to work for the employer after receiving a Final Non-confirmation (FNC) result: Employer selects this option based on the employee getting an FNC despite the employee contesting the Tentative Non-confirmation (TNC) and the employer retains the employee;
- The employee continues to work for the employer after receiving a No Show result: Employer selects this option based on the employee getting a TNC but the employee did not try to resolve the issue with SSA or DHS and the employer retains the employee;
- The employee continues to work for the employer after choosing not to contest a TNC: Employer selects this option when the employee does not contest the TNC but the employer retains the employee;
- The employee was terminated by the employer for receiving a FNC result: Employer selects this option when employee receives FNC and is terminated;
- The employee was terminated by the employer for receiving a No Show result: Employer selects this option when employee did not take an action to resolve and is terminated;
- The employee was terminated by the employer for choosing not to contest a TNC: Employer selects this option when employee does not contest the TNC and is terminated;
- The employee voluntarily quit working for the employer: Employer selects this option when employee voluntarily quits job without regard to E-Verify;
- The employee was terminated by the employer for reasons other than E-Verify: Employer selects this option when employee is terminated for reasons other than E-Verify;
- The case is invalid because another case with the same data already exists: Employer selects this option when the employer ran an invalid query because the information had already been submitted;
- The case is invalid because the data entered is incorrect: Employer selects this option when the employer ran an invalid query because the information was incorrect.

C. Information about the Employer or Designated Agent:

- Company Name
- Street Address
- Employer Identification Number
- North American Industry Classification System (NAICS) Code
- Number of Employees
- Number of Sites
- Parent Company or Corporate Company
- Name of Company Point of Contact
- Phone Number
- Fax Number
- Email Address

D. Information about the Individual Employer User of E-Verify: (e.g., Human Resource employee conducting E-Verify queries):

- Last Name
- First Name
- Middle Initial
- Phone Number
- Fax Number
- Email Address
- User ID

E. Employment Eligibility Information created by E-Verify:

- Case Verification Number
- VIS Response
  - Employment Authorized
  - SSA TNC
  - DHS TNC
  - SSA Case in Continuance (In rare cases SSA needs more than 10 federal government workdays to confirm employment eligibility)
  - DHS Case in Continuance (In rare cases DHS needs more than 10 federal government workdays to confirm employment eligibility)
  - SSA FNC
  - DHS Verification in Process
  - DHS Employment Unauthorized
  - DHS No Show
  - DHS FNC

F. Information from state Motor Vehicle Agencies (MVAs) used to verify of the information from a driver's license, permit, or state issued ID card if the state has established a MOA with DHS USCIS to allow verification of this information. The categories of records from MVAs may include:

Last Name
  - First Name
  - State or Jurisdiction of Issuance
  - Document Type
  - Document Number
  - Date of Birth
  - Status Text
  - Status Description Text
  - Expiration Date

G. Information from federal databases used to verify employment eligibility may contain some or all of the following information about the individual being verified:

  - Last Name

- First Name
- Middle Name
- Maiden Name
- Date of Birth
- Age
- Country of Birth
- Country of Citizenship
- Alien Number
- Social Security Number
- Citizenship Number
- Receipt Number
- Address
- Previous Address
- Phone Number
- Nationality
- Gender
- Photograph
- Date Entered United States
- Class of Admission
- File Control Office Code
- Form I–94 Number
- Provision of Law Cited for Employment Authorization
- Office Code Where the Authorization Was Granted
- Date Employment Authorization Decision Issued
- Date Employment Authorization Begins
- Date Employment Authorization Expires
- Date Employment Authorization Denied
- Confirmation of Employment Eligibility
- TNC of Employment Eligibility and Justification
- FNC of Employment Eligibility
- Status of Department of Justice Executive Office Immigration Review System (EOIR) Information, if in Proceedings
- Date Alien's Status Changed
- Class of Admission Code
- Date Admitted Until
- Port of Entry
- Departure Date
- Visa Number
- Passport Number
- Passport Information including COI
- Passport Card Number
- Form Number, for example Form I–551 (Lawful Permanent Resident card) or Form I–766 (Employment Authorization Document);
- Expiration Date
- Employment Authorization Card Information
- Lawful Permanent Resident Card Information
- Petitioner Internal Revenue Service Number
- Class of Admission
- Valid To Date
- Student Status
- Visa Code
- Status Code
- Status Change Date
- Port of Entry Code
- Non-Citizen Entry Date
- Program End Date
- Naturalization Certificate Number
- Naturalization Date and Place
- Naturalization Information and Certificate
- Naturalization Verification (Citizenship Certificate Identification ID)
- Naturalization Verification (Citizenship Naturalization Date/Time)
- Immigration Status (Immigration Status Code)
- Federal Bureau of Investigation Number
- Admission Number
- Petitioner Firm Name
- Petitioner Tax Number
- Date of Admission
- Marital Status
- Marriage Date and Place
- Marriage Information and Certificate
- Visa Control Number
- Visa Foil Number
- Class of Admission
- Federal Bureau of Investigation Number
- Case History
- Alerts
- Case Summary Comments
- Case Category
- Date of Encounter
- Encounter Information
- Case Actions & Decisions
- Bonds
- Current Status
- 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 United States
- File Number
- File Location

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for having a system for verification of employment eligibility is found in The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104–208 (1996).

PURPOSE(S):

This system provides employment authorization information to employers participating in E-Verify. It may also be used to support monitoring and compliance activities for obtaining information in order to prevent the commission of fraud, discrimination, or other misuse or abuse of the E-Verify system, including violation of privacy laws or other illegal activity related to misuse of E-Verify, including:

- Investigating duplicate registrations by employers;
- Inappropriate registration by individuals posing as employers;
- Verifications that are not performed within the required time limits; and
- Cases referred by and between E-Verify and the Department of Justice Office of Special Counsel for Immigration-Related Unfair Employment Practices, or other law enforcement entities.

Additionally, the information in E-Verify may be used for program management and analysis, program outreach, customer service and preventing or deterring further use of stolen identities in E-Verify.

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 the Department of Homeland Security as a routine use pursuant to 5 U.S.C. 552a(b)(3). Any disclosure of information must be made consistent with the official duties of the person making the disclosure. The routine uses are as follows:

A. To the Department of Justice (DOJ), including U.S. Attorney Offices, or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is relevant or 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.

B. To a congressional office from the record of an individual in response to a written inquiry from that congressional office made pursuant to a Privacy Act waiver from the individual to whom the record pertains.

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

D. To an agency or organization 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 employers participating in the E-Verify Program in order to verify the employment eligibility of their employees working in the United States.

I. To the American Association of Motor Vehicle Administrators Network and participating MVAs for the purpose of validating information for a driver's license, permit, or identification card issued by the Motor Vehicle Agency of states or jurisdictions who have signed a Memorandum of Agreement with DHS under the Records and Information from Departments of Motor Vehicles for E-Verify (RIDE) program.

J. To the DOJ, Civil Rights Division, for the purpose of responding to matters within the DOJ's jurisdiction of the E-Verify Program, especially with respect to discrimination.

K. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

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, verification case number, Alien Number, I–94 Number, Receipt Number, Passport (U.S. or Foreign) Number and Country of Issuance (COI), Driver's License, Permit, or State-Issued Identification Card Number, or SSN of the employee, employee user, or by the submitting company 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 E-Verify and in verifying employment eligibility are stored and retained in E-Verify for ten (10) years, from the date of the completion of the last transaction unless the records are part of an on-going investigation in which case they may be retained until completion of the investigation. This period is based on the statute of limitations for most types of misuse or fraud possible using E-Verify (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 (USCIS), Washington, DC 20528.

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 U.S. Citizenship and Immigration Services (USCIS), Freedom of Information Act (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. 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:

- Explain 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 the above 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 including:

(A) Information collected from employers about their employees relating to employment eligibility verification;

(B) Information collected from E-Verify users used to provide account access and monitoring;

(C) Information collected from Federal and state databases listed below:

- Social Security Administration Numident System
- CBP Nonimmigrant Information System (NIIS) and Border Crossing Information (BCI)
- ICE Student and Exchange Visitor Identification System (SEVIS)
- ICE ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM) Alien Number
- USCIS Aliens Change of Address System (AR–11)
- USCIS Central Index System (CIS)
- USCIS Customer Profile Management System (CPMS)
- USCIS Computer-Linked Application Information Management System Version 3 (CLAIMS 3)
- USCIS Computer-Linked Application Information Management System Version 4 (CLAIMS 4)
- USCIS Citizenship and Immigration Services Centralized Operational Repository (CISCOR)
- USCIS National File Tracking System (NFTS)
- USCIS Microfilm Digitization Application System (MiDAS)
- USCIS Marriage Fraud Amendment System (MFAS)
- USCIS Enterprise Document Management System (EDMS)
- USCIS Refugees, Asylum, and Parole System (RAPS)
- US–VISIT Arrival Departure Information System (ADIS)
- Department of State Consular Consolidated Database (CCD)
- Department of Justice Executive Office Immigration Review System (EOIR) State Motor Vehicle Administrations, if participating in the E-Verify RIDE initiative.

(D) Information created by E-Verify.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: July 27, 2012.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2012–19204 Filed 8–7–12; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG—2012—0763]

Merchant Marine Personnel Advisory Committee

AGENCY: Coast Guard, DHS.

ACTION: Notice of Federal Advisory Committee Meeting.

SUMMARY: The Merchant Marine Personnel Advisory Committee (MERPAC) will meet in Washington, DC, to discuss various issues related to the training and fitness of merchant marine personnel. This meeting will be open to the public.

DATES: MERPAC working groups will meet on September 11, 2012, from 8 a.m. until 4 p.m., and the full committee will meet briefly on the morning of September 11 and on September 12, 2012, from 8 a.m. until 4 p.m. This meeting may adjourn early if all business is finished. Written comments to be distributed to committee members and placed on MERPAC's Web site are due August 31, 2012.

ADDRESSES: The Committee will meet in Room 2501 of the U.S. Coast Guard Headquarters Building, 2100 Second Street SW., Washington, DC 20593. Attendees will be required to provide a picture identification card and pass through a magnetometer in order to gain admittance to the U.S. Coast Guard Headquarters Building. Visitors should also arrive at least 30 minutes in advance of the meeting in case of long lines at the entrance.

For information on facilities or services for individuals with disabilities or to request special assistance, contact Mr. Rogers Henderson at 202–372–1408 as soon as possible.

To facilitate public participation, we are inviting public comment on the issues to be considered by the Committee and working groups as listed in the ''Agenda'' section below. Written comments must be identified by Docket No. USCG–2012–0763 and submitted by one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments (preferred method to avoid delays in processing).
- *Fax:* 202–372–1918.
- *Mail:* Docket Management Facility (M–30), U.S. Department of Transportation, West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue SE., Washington, DC 20590–0001.
- *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.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. Comments received will be posted without alteration at *http://www.regulations.gov*, including any personal information provided. You may review a Privacy Act notice regarding our public dockets in the January 17, 2008, issue of the **Federal Register** (73 FR 3316).

Docket: For access to the docket to read documents or comments related to this notice, go to *http://www.regulations.gov*.

Any requests to make oral presentations should be made in advance using one of the methods highlighted above. This notice may be viewed in our online docket, USCG–2012–0763, at *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: Mr. Rogers Henderson, Alternate Designated Federal Officer (ADFO), telephone 202–372–1408. If you have any questions on viewing or submitting material to the docket, call Renee V. Wright, Program Manager, Docket Operations, telephone 202–366–9826.

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the *Federal Advisory Committee Act,* 5 U.S.C. App. (Pub. L. 92–463).

MERPAC is an advisory committee established under the Secretary's authority in section 871 of the Homeland Security Act of 2002, Title 6, United States Code, section 451, and chartered under the provisions of the FACA. The Committee acts solely in an advisory capacity to the Secretary of the Department of Homeland Security (DHS) through the Commandant of the Coast Guard and the Director of Commercial Regulations and Standards on matters relating to personnel in the U.S. merchant marine, including but not limited to training, qualifications, certification, documentation, and fitness standards. The Committee will advise, consult with, and make