RETRIEVABILITY:

NOAD information maintained in SANS is not retrievable by name or other unique personal identifier. NOAD information is extracted from SANS by vessel and then retrieved by name, passport number, or other unique personal identifier.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include role-based access provisions, restricting access to authorized personnel who have a need-to-know, using locks, and password protection identification features. USCG file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel.

The system manager, in addition, has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations.

All communication links with the USCG datacenter are encrypted. The databases are Certified and Accredited in accordance with the requirements of the Federal Information Security Management Act (FISMA).

RETENTION AND DISPOSAL:

Information on vessels maintained in SANS is destroyed or deleted when no longer needed for reference, or when ten years old, whichever is later. [National Archives and Records Administration (NARA) Request For Records Disposition Authority, Job No. N1–026–05–11]

Outputs, which include ad-hoc reports generated for local and immediate use to provide a variety of interested parties, for example, Captain of the Port and marine safety offices, sea marshals, Customs and Border Patrol (CBP), Immigration and Customs Enforcement (ICE)—with the necessary information to set up security zones, scheduling boarding and inspections activities, actions for non-compliance with regulations, and other activities in support of CG's mission to provide for safety and security of U.S. ports, will be deleted after five years if it is not a permanent record according to NARA.

The only NOAD information retained based initially on SANS data is information related to those individuals about whom derogatory information is revealed during the screening process. All other crew and passenger information vetted by USCG is immediately deleted. Should derogatory information be discovered by USCG either through TECS or USCG's own sources, such alerts and information would be communicated either through USCG's Maritime Awareness Global Network (MAGNet) system, or through the Coast Guard Messaging System (CGMS).[2] This information will be maintained for the life of the investigation or ten years, which ever is longer. The SANS data is transmitted to the ICC and stored in the CP3. SANS data within CP3 is destroyed or deleted when no longer needed for reference, or when ten years old, whichever is later.

SYSTEM MANAGER(S) AND ADDRESS:

Commandant, CG–26, United States Coast Guard Headquarters, 2100 2nd Street, SW., Washington, DC 20593–0001.

NOTIFICATION PROCEDURES:

To determine whether this system contains records relating to you, write to the System Manager identified above. Your written request should include your name and mailing address. You may also provide any additional information that will assist in determining if there is a record relating to you if applicable, such as your Merchant Mariner License or document number, the name and identifying number (documentation number, state registration number, International Maritime Organization (IMO) number, etc.) of any vessel with which you have been associated and the name and address of any facility (including platforms, deep water ports, marinas, or terminals) with which you have been associated. The request must be signed by the individual, or his/her legal representative, and must be notarized to certify the identity of the requesting individual pursuant to 28 U.S.C. 1746 (unsworn declarations under penalty of perjury). Submit a written request identifying the record system and the category and types of records sought to the Executive Agent. Request can also be submitted via the FOI/Privacy Acts. See *http://www.uscg.mil/foia/* for additional information.

RECORD ACCESS PROCEDURES:

Write the System Manager at the address given above in accordance with the ''Notification Procedure''. Provide your full name and a description of the information you seek, including the time frame during which the record(s) may have been generated. Individuals requesting access to their own records must comply with DHS's Privacy Act regulation on verification of identity (6 CFR 5.21(d)). Further information may also be found at *http://www.dhs.gov/foia* or at *http://www.uscg.mil/foia/*.

CONTESTING RECORD PROCEDURES:

See ''Notification'' procedures above.

RECORD SOURCE CATEGORIES:

The system contains data received from vessel carriers and operators regarding passengers and crewmembers who arrive in, depart from, transit through the U.S. on a vessel carrier covered by notice of arrival and departure regulations.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

This system, however, may contain records or information recompiled from or created from information contained in other systems of records, which are exempt from certain provisions of the Privacy Act. For these records or information only, in accordance with 5 U.S.C. 552a (j)(2),(k) (1), and (k)(2), DHS will also claim the original exemptions for these records or information from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect such information.

Dated: December 2, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29279 Filed 12–10–08; 8:45 am]

BILLING CODE 4410–10–P

[2] *See www.dhs.gov/privacy* for PIAs for MAGNet and the Law Enforcement Intelligence Database (LEIDB), a system used to analyze USCG message traffic.

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0089]

Privacy Act of 1974; USCIS–004 Verification Information System (VIS) System of Records Notice

AGENCY: Privacy Office, DHS.

ACTION: Notice to alter a Privacy Act system of records.

SUMMARY: The Department of Homeland Security (DHS) is republishing the Privacy Act system of records notice (SORN) for the Verification and Information System (VIS) replacing the previously published SORN of February 28, 2008 in order to: (1) Cover the expansion of VIS to collect and verify

United States (U.S.) Passports and Passport Cards from E-Verify users, (2) describe the expansion of the scope of the Systematic Alien Verification for Entitlements (SAVE) to include verification of citizenship and immigration status for any DHS lawful purpose, not just for government benefit granting purposes as described in previous PIAs, (3) cover the expansion of VIS to collect applications from victims of identity theft who would like to lock their Social Security Number (SSN) from further use in E-Verify, and (4) describe the expansion of the scope of E-Verify to indicate that it is no longer solely voluntary in some cases and no longer solely for new employees. These changes are more thoroughly spelled out in an accompanying Privacy Impact Assessment (PIA) which can be found on the DHS Privacy Web site (*http://www.dhs.gov/privacy*).

DATES: Written comments must be submitted on or before January 12, 2009.

ADDRESSES: You may submit comments, identified by Docket Number DHS–2008–0089 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.
- *Fax:* 1–866–466–5370.
- *Mail:* Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528.
- *Instructions:* All submissions received must include the agency name and docket number for this system of records notice. 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 additional information on the program please contact: Claire Stapleton, Privacy Branch Chief, Verification Division, U.S. Citizenship and Immigration Services, Department of Homeland Security, 470 L'Enfant Plaza East, SW., Suite 8204, Washington, DC 20529. For privacy issues please contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. USCIS Verification Information System

Congress mandated that USCIS establish a system that can be used to verify citizenship and immigration status of individuals seeking government benefits and establish a system for use by employers to determine whether an employee is authorized to work in the United States. 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), Pub. L. 104–193, 110 Stat. 2168, and in Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104–208, 110 Stat. 3009. Authority for having a system establish employment eligibility can be found in Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104–208, 110 Stat. 3009. The Basic Pilot Program's operation has been repeatedly extended by Congress; See Basic Pilot Extension Act, Public Law 107–128 (2002); Basic Pilot Program Extension and Expansion Act, Public Law 108–156 (2003); Consolidated Security, Disaster Assistance, and Consolidated Appropriations Act, 2009, Public Law 110–329 (2008).

USCIS implemented these mandates through the Systematic Alien Verification for Entitlements (SAVE) program for government benefits and the ''Basic Pilot Program'' for determining whether an employee is authorized to work in the United States. The ''Basic Pilot Program'' was renamed ''E-Verify.'' ''E-Verify'' will be used in lieu of ''Basic Pilot'' for the remainder of this document.

VIS is the technical infrastructure that enables USCIS to operate SAVE and E-Verify. VIS is a nationally accessible database of selected immigration status information containing in excess of 100 million records. Previously government agencies used information from the SAVE program in order to determine whether an individual is eligible for any public benefit, license or credential based on individual's citizenship or immigration status. This SORN describes expansions to the SAVE program. Private employers and government users use E-Verify to confirm whether an employee is authorized to work in the United States.

A necessary corollary to having the ability to determine if an individual is authorized to gain government benefits or legal employment is the ability to determine if the verification processes are being abused or misused: And when appropriate, to seek legal or administrative redress against those committing fraud or otherwise misusing the verification processes. Consequently, the information in VIS is retained and analyzed for ten years, the length of time equivalent to the statute of limitations for the most typical types of fraud or misuse of this type of system or documents (under 18 U.S.C. 3291, the statute of limitations for false statements or misuse regarding passports, citizenship or naturalization documents), or longer if the information is part of an active and ongoing investigation.

VIS is currently comprised of citizenship, immigration and employment status information from several DHS systems of records, including records contained in the U.S. Customs and Border Protection (CBP) Treasury Enforcement Communication Systems (TECS) (66 FR 52984), Biometric Storage System (BSS) (72 FR 17172), the USCIS Central Index System (CIS) (72 FR 1755), the USCIS Computer Linked Application Information Management System (CLAIMS 3) (62 FR 11919) and Immigration and Customs Enforcement's (ICE) Student and Exchange Visitor Information System (SEVIS) (70 FR 14477). VIS also includes information from the Social Security Administration's (SSA) NUMIDENT System (71 FR 1796).

This System of Records Notice is replacing the System of Records Notice previously published in the **Federal Register** on February 28, 2008 (73 FR 10793).

A. SAVE Program

The SAVE Program, which is supported by VIS, has previously been characterized as being limited to immigration and citizenship status verification for purposes of eligibility for any public benefit, license or credential—the benefit or ''entitlement'' referred to in the name of the program: Systematic Alien Verification for Entitlements (SAVE). However, section 642(c) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) 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''.

Accordingly, to the extent that a federal, state, or local government entity has the legal authority to verify citizenship or immigration status, SAVE, as an access method to USCIS systems, is authorized to respond to the request. Specifically, in addition to the

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 VIS for status determinations. If VIS has a record pertaining to the individual, the government agency will receive limited biographic information on the citizenship and immigration status of the individual. If VIS does not have a record pertaining to the individual, VIS automatically notifies a USCIS employee. The USCIS employee then conducts a manual search of other DHS databases to determine whether there is any other information pertaining to that individual that would provide verification of citizenship and immigration status. If the USCIS employee finds additional relevant information, citizenship and immigration status data is provided to the requesting government agency user through VIS. The USCIS employee will also update the appropriate record in the USCIS CIS database. The REAL ID Act of 2005, Public Law 109–13, 119 Stat. 231, 302 (2005) (codified at 49 U.S.C. 30301 note) required all state Departments of Motor Vehicles (DMV) to routinely utilize the USCIS SAVE program to verify the legal immigration status of applicants for driver's licenses and identification cards. The Act originally set a deadline of May 11, 2008 for states to begin such verifications, but that deadline has been extended by Congress.

B. E-Verify

VIS also supports the E-Verify Program, a free program allowing participating employers to verify the employment eligibility of their employees. The program is a collaboration between the SSA and USCIS.

After an individual is hired by an employer participating in E-Verify and the individual completes the Employment Eligibility Verification Form I–9, the employer inputs information from sections 1 and 2 of the Form I–9 into the E-Verify portion of VIS. This query is first sent from VIS to SSA to verify Social Security information. If SSA cannot verify the employee's social security information, SSA will send a SSA Tentative Non-Confirmation (TNC) response to VIS, which in turn will notify the employer of SSA's inability to automatically verify the information provided by employee. The employer is then required to provide information to the employee about the employee's option to contest and the contact information for the SSA office in order to clear up the mismatch and resolve any issues.

If SSA is able to verify the employee information and the individual is a non-U.S. citizen, the VIS system continues the process by comparing the non-U.S. citizen's information with USCIS records to verify employment authorization. For any participating employer whose non-U.S. citizen employees present an I–551 or I–766 card for their Form I–9 documentation and whose information is successfully verified by SSA and USCIS, the employer will be able to use the USCIS photo tool to compare the photographs on the documents presented by the employee with the photographs and stored in the BSS system of records, if available. If VIS is able to return a photograph, the employer will then compare the photograph made available by the VIS photo tool and determine if it matches the photograph on the document presented by the employee. If the employer determines the photos do not match or if the employer cannot make a determination whether there is a photo match, the employer is then required to provide information to the employee about how the employee may contact USCIS to resolve any issues.

After the process of verifying the employment authorization concludes, regardless of whether or not the photo tool has been utilized, USCIS (through VIS) provides the employer with a case verification number and the disposition of whether an employee has been verified to be authorized to work. If a mismatch of information occurs with DHS, VIS automatically notifies an USCIS employee, who then conducts a manual search of other DHS databases to determine whether there is any other information pertaining to that individual that would help to establish employment authorization. If the USCIS employee cannot determine the person's work authorization, VIS sends a ''DHS Tentative Non-Confirmation'' (TNC) response notifying the employer that the employee has the option to contact USCIS in order to clarify the information discrepancy. DHS TNCs are issued when the USCIS employee is unable to determine the person's work authorization based on DHS immigration-related records. The employer may not terminate or take any adverse employment action against the employee on the basis of either a DHS or SSA TNC while the issue is being further investigated. If a Final Non-Confirmation (FNC) response is issued, the employer may terminate the employee or they may choose to retain the employee as long as the employer notifies DHS that it intends to do so, subject to potential penalties if the employee is subsequently found to be an unauthorized alien. If the employer does not choose to retain the employee after receiving a Final Non-Confirmation response it is not required to notify DHS.

Performing a verification query through the E-Verify system is only permissible after an offer of employment has been extended to an employee. The earliest the employer may initiate a query is after an individual accepts an offer of employment and after the employee and employer complete the Form I–9. For new employees, the employer must initiate the query no later than the end of the third business day after the new hire's actual start date. Under the terms governing employers' participation in E-Verify, the system cannot be used to pre-screen job applicants or to re-screen individuals whose work eligibility has already been confirmed by the employer through E-Verify.

C. Changes to VIS SORN

This SORN is being published to: (1) Cover the expansion of VIS to collect and verify information from U.S. Passports and Passport Cards from E-Verify users; (2) describe the expansion of the scope of SAVE to include verification of citizenship and immigration status for any DHS lawful purpose, not just for government benefit granting purposes as described in previous PIAs; (3) cover the expansion of VIS to collect applications from victims of identity theft who would like to lock their SSN from further use in E-Verify; and (4) describe the expansion of the scope of E-Verify to indicate that it is no longer solely voluntary in some cases and no longer solely for new employees in certain cases.

Expansion of VIS To Collect and Verify United States Passports and Passport Cards

E-Verify is used to determine whether an individual is authorized to work in the U.S. An employer who participates in E-Verify uses the information that they have previously collected for the Form I–9 process. Thus a U.S. citizen may present a Passport or Passport Card for purposes of proof of employment authorization for the Form I–9. The Passport Card is a new identity document issued by the Department of State (DOS) that will act as a passport in limited circumstances and will be acceptable for use in place of a U.S. passport for Form I–9 and E-Verify purposes. The information contained on

the Passport Card is the same information in the passport other than the document identification number. It is possible to have a U.S. Passport and a Passport Card. The numbers on the two documents would not be the same. The U.S. Passport and the Passport Card can both be used to establish identity and work authorization for Form I–9 purposes. Currently, an E-Verify employer captures the passport information (if presented as a List A document) from an employee; however, prior to this update the VIS system neither captured nor confirmed the passport number against government-held data.

Regardless of the identity document presented to the employer for the Form I–9, the VIS system requires an employee's Social Security Number (SSN) to verify employment eligibility. With this update, if an employee presents a U.S. Passport or Passport Card, VIS will initially check the employee's identity information, including Name, Date of Birth, citizenship status, and SSN, against the Social Security Administration (SSA) database; however, if the Social Security Administration (SSA) cannot verify the employee's citizenship status information, then VIS will verify the employee's Passport or Passport Card data against DOS data using an existing interface with Customs and Border Protection's (CBP) Treasury Enforcement Communications System (TECS). It may not be possible to determine an employee's work authorization solely through a query to the SSA database, for example, because SSA may not have been informed that an immigrant has become a U.S. citizen. Previously, such an inability to verify would have resulted in requiring the employee to visit an SSA Field Office and clarify citizenship status with the SSA. If the SSN is verified, VIS will verify the Passport number or Passport Card number so that an employer can have the capability to visually compare the photograph that appears on a Passport or Passport Card with the photograph that DOS has on file. E-Verify provides access to this information through the Photo Screening Tool which is described in the PIA published September 4, 2007. VIS will not retain a copy of the photograph as provided from the DOS data, merely a link that can be followed to retrieve the photograph in TECS should it need to be validated later. However, VIS may retain a hard copy of the photograph when an initial verification cannot be done by the employer and a secondary verification has to be done by the Verification Division Status Verifiers. This is the same procedure followed for other documents where the initial verification cannot be done by the employer.

Expansion of SAVE for Verification of Citizenship and Immigration Status

SAVE has previously been characterized as being limited to immigration and citizenship status verification for purposes of eligibility for any public benefit, license or credential—the benefit or ''entitlement'' is referred to in the name of the program Systematic Alien Verification for Entitlements (SAVE). However, section 642(c) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) 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.''

Accordingly, to the extent that a federal, state, or local government entity has the legal authority to verify citizenship or immigration status, SAVE, as an access method to USCIS systems, is authorized to respond to the request. Specifically, in addition to the verifications for purposes of granting government benefits, this includes verification for purposes of legally mandated background investigations. These legally mandated background investigations might be conducted by the OPM or other government entities where determination of immigration status is relevant to the reason for conducting the investigation, such as for Federal personnel security clearances or staff in sensitive critical infrastructure facilities in the private sector. For certain security clearances OPM may verify not only the individuals who are the subject of the background investigations, but also their family members and cohabitants (associated individuals) based on information the SAVE applicant provides to OPM. The associated individuals who are being verified through SAVE will only have notice of the verification by means of this SORN and accompanying PIA.

Expansion of VIS To Collect Application Information From Those Who Choose To Lock Their SSN From Further Use in E-Verify

JobLock is one part of an on-going effort by the Department of Homeland Security (DHS) to fight identity theft. This particular effort is targeted at victims of identity theft that have filed both a police report and a complaint with the Federal Trade Commission regarding identity theft that has been perpetrated against them. These victims will be given the opportunity to apply to USCIS to have their social security number (SSN) locked from further use in E-Verify. The application will be accessible through USCIS's E-filing system, and applicants will provide information to USCIS that will be validated against Federal Trade Commission's (FTC) Consumer Sentinel Database. The applicant is also required to provide USCIS with a copy of the police report issued by their local police jurisdiction. Once a JobLock application has been validated by a USCIS employee, a database table within VIS of locked SSNs (JobLock Table) will be populated, which will contain the SSN, the JobLock application information, and account information necessary to unlock the SSN (*i.e.* challenge questions and answers.)

Regardless of the identity document presented to the employer for the Form I–9, the VIS system requires an employee's SSN to verify employment eligibility. After the query information (name, date of birth, citizenship status, and SSN) has been verified by SSA, the system will check against the JobLock Table to verify whether the SSN has been locked from further use in E-Verify. If the SSN is not found in the JobLock Table, the query will be processed in the same manner it has been in the past. If the SSN queried upon is found in the JobLock Table, a DHS tentative non-confirmation would be issued by the system and the employee would be directed to contact a USCIS employee. The locking of an SSN will prevent an identity thief from using it to establish employment eligibility with E-Verify.

Change in the Scope of E-Verify

E-Verify, including its original iteration as Basic Pilot, has operated to date as a program for employers to verify employment eligibility of their new employees. Employers have not been permitted to verify the employment eligibility of existing employees. Recently, several state and Federal laws have required employer participation in the program for new hires in various circumstances. These laws range from some states requiring that all employers in that state participate in E-Verify, to other states requiring the state contractor workforce or government employers to participate. In addition, the Federal government requires that all newly-hired Federal employees be verified through E-Verify, and has adopted a federal procurement policy of contracting only with

employers that agree to use E-Verify to verify the work authorization of their new employees as well as all employees assigned to work on federal contracts. As a result, the population of E-Verify users has expanded, and will continue to expand. E-Verify will also begin to be used for some employers' existing workforce in addition to newly hired employees.

II. The 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 personally identifiable information. 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 from which information is retrieved by the name of an individual or by some identifying number, symbol, or other particular assigned to an individual.

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 to make agency recordkeeping practices transparent, to notify individuals reading the uses to which personally identifiable information is put, and to assist the individual to more easily find such files within the agency.

III. Privacy Impact Assessments

DHS is publishing a PIA update to coincide with this SORN. This SORN reflects many of the changes that are discussed in this PIA.

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

System of Records: DHS/USCIS–004

SYSTEM NAME:

U.S. Citizenship and Immigration Services Verification Information System (VIS).

SYSTEM LOCATION:

The Verification Information System (VIS) database is housed in a contractor-owned facility in Meriden, CT. The system is accessible via the Internet, Web services, Secure File Transfer Protocol (SFTP) batch, and through a computer via analog telephone line, and is publicly accessible to participants of the SAVE program and the E-Verify program, including authorized USCIS personnel, other authorized government users, participating employers, and other authorized users.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system contains information on individuals, both U.S. citizens and non-U.S. citizens covered by provisions of the Immigration and Nationality Act of the United States including but not limited to individuals who have been lawfully admitted to the United States, individuals who have been granted U.S. citizenship and individuals who have applied for other immigration benefits pursuant to 8 U.S.C. 1103 *et seq.* In addition, it contains information on cohabitants and relatives of subjects of SAVE background investigations conducted for OPM. This system also contains information on individuals, both U.S. citizens and non-U.S. citizens, whose employers have submitted to the E-Verify program their identification information. This system also contains information on individuals, both U.S. citizens and non-U.S. citizens, who have been victims of identity theft and have chosen to lock their Social Security number from further use in the E-Verify program.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Data originating from the USCIS Central Index System (CIS), including the following information about the individual who comes before USCIS: Alien Registration Number (A-Number), Name (last, first, middle), Date of birth, Date entered United States (entry date), Country of birth, Class of Admission code, File Control Office code, Social Security Number, Admission Number (I–94 Number), Provision of Law code cited for employment authorization, office code where the authorization was granted, Date employment authorization decision issued, Date employment authorization may begin (start date), Date employment authorization expires (expiration date), and Date employment authorization was denied (denial date).

B. Data originating from the U.S. Customs and Border Protection Treasury Enforcement Communications System (TECS), including the following information about the individual: A-Number, Name (last, first, middle), Date alien's status was changed (status change date), Date of birth, Class of Admission Code, Date admitted until, Country of citizenship, Port of entry, Date entered United States (entry date), Departure date, I–94 Number, Visa Number, and transaction link to passport photographs contained in TECS.

C. Data originating from the Redesigned Naturalization Automated Casework System (RNACS). RNACS is a database that includes information from individuals who have filed applications for naturalization, citizenship, or to replace naturalization certificates under the Immigration and Nationality Act, as amended, and/or who have submitted fee payments with such applications. The naturalization records in the RNACS database house information from 1986 to 1996. Information that identifies individuals named above, e.g., Name, Address, Date of birth, and Alien Registration Number (A-Number). Records in the system may also include information such as Date documents were filed or received in CIS, Status, Class of admission codes, and Locations of record.

D. Data originating from the Computer Linked Applications Information Management System (CLAIMS 4) including the following information about the individual; Name (First, Last), Date of birth, Social Security Number, and Naturalization date.

E. Data originating from the USCIS Biometric Storage System (BSS), including: Receipt number, Name (last, first, middle), Date of birth, Country of birth, Alien Registration Number (A-Number), Form number, for example Form I–551 (Lawful Permanent Resident card) or Form I–766 (Employment Authorization Document), Expiration date, and Photo.

F. Data originating from the USCIS Computer Linked Application Information Management System (CLAIMS 3), including: Receipt number, Name (last, first, middle), Date of birth, Country of birth, Class of admission code, Alien Registration Number (A-Number), I–94 number, Date entered United States (entry date), and Valid-To Date.

G. Data originating from the U.S. Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Information System (SEVIS), including: SEVIS Identification Number (SEVIS ID), Name (last, first, middle), Date of birth, Country of birth, Class of admission code, I–94 number, Date entered United States (entry date), and Valid-to Date.

H. Data originating from the Social Security Administration (SSA), including: Confirmation of employment eligibility based on SSA records, Tentative non-confirmation of employment eligibility and the underlying justification for this decision, and Final non-confirmation of employment eligibility.

I. Information collected from the benefit applicant by a federal, state, local or other benefit-issuing agency to facilitate immigration status verification

that may include the following about the benefit applicant: Receipt Number, A-Number, I–94 Number, Name (last, first, middle), Date of birth, User Case Number, DHS document type, DHS document expiration date, SEVIS ID and Visa Number.

J. Information collected from the benefit-issuing agency about users accessing the system to facilitate immigration status verification that may include the following about the agency: Agency name, Address, Point(s) of Contact, Contact telephone number, Fax number, E-mail address, Type of benefit(s) the agency issues (i.e. Unemployment Insurance, Educational Assistance, Driver Licensing, Social Security Enumeration, etc.).

K. Information collected from the benefit-issuing agency about the Individual Agency User including: Name (last, first, middle), Phone Number, Fax Number, E-mail address, User ID for users within the Agency.

L. System-generated response, as a result of the SAVE verification process including: Case Verification Number, Entire record in VIS database as outlined above, including all information from CIS, SEVIS, TECS, and CLAIMS 3 and with the exception of the biometric information (photo) from BSS, and Immigration status (e.g. Lawful Permanent Resident).

M. Information collected from the employee by the Employer User to facilitate employment eligibility verification may include the following about the Individual employee: Receipt Number, Visa Number, United States or Foreign Passport number, Passport Card number, Alien Registration Number (A-Number), I–94 Number, Name (last, first, middle initial, maiden), Social Security Number, Date of birth, Date of hire, Claimed citizenship status, Acceptable Form I–9 document type, Acceptable Form I–9 Document expiration date, and Passport, Passport Card, or visa photo.

N. Information Collected About the Employer, including: Company name, Physical Address, Employer Identification Number, North American Industry Classification System code, Federal contracting agency, Federal contract identifier, Number of employees, Number of sites, Parent company or Corporate company, Name of Contact(s), Phone Number, Fax Number, and E-Mail Address.

O. Information Collected about the Employer User (e.g., Identifying users of the system at the Employers), including: Name, Phone Number, Fax Number, E-mail address, and User ID.

P. System-generated response information, resulting from the E-Verify employment eligibility verification process, including: Case Verification Number; VIS generated response: Employment authorized, Tentative non-confirmation, Case in continuance, Final non-confirmation, Employment unauthorized, or DHS No Show; Disposition data from the employer includes Resolved Unauthorized/ Terminated, Self Terminated, Invalid Query, Employee not terminated, Resolved Authorized, and Request additional verification, which includes why additional verification is requested by the employer user.

Q. Information collected directly from individuals who have been the victim of identity theft who wish to prevent or deter further use of stolen identities in E-Verify, including: Police reports, Name, Social Security Number, Street address, E-mail address, and Other identity authentication information relevant to preventing or deterring further use of stolen identities.

AUTHORITY FOR MAINTENANCE OF RECORDS:

The authority for the maintenance of records in the system is found in 8 U.S.C. 1324a, 8 U.S.C. 1360, 42 U.S.C. 1320b–7 and 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 in Executive Order 12989, as amended by Executive Order 13465, June 6, 2008.

PURPOSE(S):

This system of records is used to provide immigration and citizenship status information to Federal, State, and local government agencies on any individual within the jurisdiction of the requesting agency, or on another individual associated with such an individual, for any purpose authorized by law. It is also used to provide employment authorization information to employers participating in the E-Verify Program. This system of records may also be used to monitor for the commission of fraud or other illegal activity related to misuse of either the SAVE or E-Verify program, 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 to E-Verify or SAVE by the Department of Justice (DOJ) Office of Special Counsel for Immigration-Related Unfair Employment Practices (OSC). This system of records may also be used for 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, 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 a federal, state, tribal, or local government agency, or to a contractor acting on the agency's behalf, to the extent that such disclosure is necessary to enable these agencies to make decisions concerning: (1) Determination of eligibility for a federal, state, or local public benefit; (2) issuance of a license or grant; (3) government-issued credential; or (4) background investigation.

B. To employers participating in the E-Verify Employment Verification Program in order to verify the employment eligibility of their employees working in the United States.

C. To other Federal, State, tribal, and local government agencies seeking to verify or determine the citizenship or immigration status of any individual within the jurisdiction of the requesting agency as authorized or required by law.

D. To contractors, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish a DHS mission function related to this system of records, in compliance with the Privacy Act of 1974, as amended.

E. 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.

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

G. To a former employee of the Department for purposes of: (1) Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or (2) facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee

regarding a matter within that person's former area of responsibility.

H. To the DOJ, Civil Rights Division, for the purpose of responding to matters within the DOJ's jurisdiction to include allegations of fraud and/or nationality discrimination.

I. To appropriate agencies, entities, and persons when: (1) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) it is 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) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons when reasonably necessary to assist in connection with efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

J. To the United States Department of Justice (including United States Attorney offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, or to the court 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; (2) any employee of DHS in his or her official capacity; (3) any employee of DHS in his or her individual capacity where DOJ or DHS has agreed to represent said employee; or (4) the United States or any agency thereof;

K. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

L. To the Federal Trade Commission (FTC) to validate against the FTC's Consumer Sentinel Database.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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

STORAGE:

Data is stored in computer accessible storage media and hardcopy format.

RETRIEVABILITY:

Agency records are retrieved by name of applicant or other unique identifier to include: verification number, A-Number, I–94 Number, Visa Number, SEVIS ID, or by the submitting agency name. Employer records are retrieved by verification number, A-Number, I–94 Number, Receipt Number, Passport (U.S. or Foreign) number or Social Security Number of the employee, or by the submitting company name.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws and policies, including the DHS information technology security policies and the Federal Information Security Management Act (FISMA). All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel on a need-to-know basis, using locks, and password protection features. The system is also protected through a multi-layer security approach. The protective strategies are physical, technical, administrative and environmental in nature, which provide access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication of sending parties, and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties. Information maintained by DHS contractors for this system is also safeguarded in accordance with all applicable laws and regulations, including DHS IT security policies and FISMA. Access is controlled through user identification and discrete password functions to assure that accessibility is limited.

RETENTION AND DISPOSAL:

The following proposal for retention and disposal is being prepared to be sent to the National Archives and Records Administration for approval. Records collected in the process of establishing immigration and citizenship status or employment authorization are stored and retained in the VIS Repository for ten (10) years, from the date of the completion of the verification 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 VIS (under 18 U.S.C. 3291, the statute of limitations for false statements or misuse regarding passports, citizenship or naturalization documents). Records related to the prevention or deterrence of identity theft that are collected from individuals who voluntarily provide the information or that is obtained with the authorization of victims and potential victims of identity theft may be stored and retained in the VIS repository for the duration of the risk of identity theft, subject to the consent of the individual that authorized the collection. Such renewed consent shall be sought biannually.

Once the Web user views the photo, the image is discarded and not retained on the Web user's computer. Photocopies mailed to DHS in response to a TNC will be maintained as long as necessary to complete the verification process, and the duration of the benefit granted, but not limited to possible investigation and prosecution of fraud in the case of detected photo substitution.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Verification Division, U.S. Citizenship and Immigration Services, 470–490 L'Enfant Plaza East, SW., Suite 8206, Washington, DC 20024.

NOTIFICATION PROCEDURES:

Please address your inquiries about the VIS system in writing to the system manager identified above. To determine whether this system contains records relating to you, provide a written request containing the following information:

1. Identification of the record system;

2. Identification of the category and types of records sought; and

3. The requesting individual's signature and verification of identity pursuant to 28 U.S.C. 1746, which permits statements to be made under penalty of perjury. Alternatively, a notarized statement may be provided.

Address inquiries to the system manager at: Chief, Verification Division, U.S. Citizenship and Immigration Services, 470–490 L'Enfant Plaza East, SW., Suite 8206, Washington, DC 20024, or to the Freedom of Information/Privacy Act Office, USCIS, National Records Center, P.O. Box 6481010, Lee Summit, MO 64064–8010.

RECORD ACCESS PROCEDURES:

In order to gain access to one's information stored in the VIS database, a request for access must be made in writing and addressed to the Freedom of Information Act/Privacy Act (FOIA/PA) officer at USCIS. Individuals who are seeking information pertaining to them

are directed to clearly mark the envelope and letter ''Privacy Act Request.'' Within the text of the request, the subject of the record must provide his/her account number and/or the full name, date and place of birth, and notarized signature, and any other information which may assist in identifying and locating the record, and a return address. For convenience, individuals may obtain Form G–639, FOIA/PA Request, from the nearest DHS office and used to submit a request for access. The procedures for making a request for access to one's records can also be found on the USCIS Web site, located at *http://www.uscis.gov*.

An individual who would like to file a FOIA/PA request to view their USCIS record may do so by sending the request to the following address: U.S. Citizenship and Immigration Services, National Records Center, FOIA/PA Office, P.O. Box 648010, Lee's Summit, MO 64064–8010.

CONTESTING RECORDS PROCEDURES:

Individuals have an opportunity to correct their data by submitting a redress request directly to the USCIS Privacy Officer who refers the redress request to the USCIS Office of Records. When a redress request is made, any appropriate change is added directly to the existing records stored in the underlying DHS system of records from which the information was obtained. Once the record is updated in the underlying DHS system of records, it is downloaded into VIS. If an applicant believes their file is incorrect but does not know which information is erroneous, the applicant may file a Privacy Act request to access their record as detailed in the section titled ''Record access procedures'' above.

RECORD SOURCE CATEGORIES:

Information contained comes from several sources: (A) Information derived from the following DHS systems of records, USCIS's CIS, CLAIMS3, CLAIMS4, RNACS, ISRS and/or BSS (when the latter system is deployed); CBP's TECS; and ICE's SEVIS, (B) Information derived from the SSA, (C) Information collected from agencies and employers about individuals seeking government benefits or employment with an employer using an employment verification program, (D) Information collected from system users at either the agency or the employer used to provide account access to the verification program, and (E) Information developed by VIS to identify possible issues of misuse or fraud.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: December 2, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29283 Filed 12–10–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0131]

Privacy Act of 1974; United States Immigration and Customs Enforcement-009 External Investigations 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 is giving notice that it proposes to consolidate two legacy record systems originally published by the legacy Customs Service: Treasury/CS.129 Investigations Record System, October 18, 2001, and Treasury/CS.285 Automated Index to Central Investigative Files, October 18, 2001, into a Immigration and Customs Enforcement system of records notice titled External Investigations. In addition, DHS will now cover those Immigration and Customs Enforcement records previously covered by the Treasury/CS.244 Treasury Enforcement Communications System with this new system of records. Categories of individuals, categories of records, and the routine uses of these legacy system of records notices have been consolidated and updated to better reflect the law enforcement investigatory records maintained by Immigration and Customs Enforcement. Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) concurrent with this SORN elsewhere in the **Federal Register**. The exemptions for the legacy system of records notices will continue to be applicable until the final rule for this SORN has been completed This system will be included in the Department's inventory of record systems.

DATES: Written comments must be submitted on or before January 12, 2009. This new system will be effective January 12, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0131 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 1–866–466–5370.
- *Mail:* Hugo Teufel III, 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 and may be read at *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 issues please contact Lyn Rahilly, Privacy Officer, (202–731–3300), Immigration and Customs Enforcement, 500 12th Street, SW., Washington, DC 20024, e-mail: *ICEPrivacy@dhs.gov.* For privacy issues please contact Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

Immigration and Customs Enforcement (ICE) is the largest investigative branch of the Department of Homeland Security (DHS). The agency was created after 9/11, by combining the law enforcement arms of the former Immigration and Naturalization Service (INS) and the former Customs Service, to more effectively enforce our immigration and customs laws and to protect the United States against terrorist attacks. ICE does this by targeting the people, money and materials that support terrorism and other criminal activities. ICE investigates on its own and in conjunction with other agencies a broad range of illegal activities, such as terrorism, organized crime, gangs, child exploitation, and intellectual property violations.

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107–296, Section 1512, 116 Stat. 2310 (Nov. 25, 2002), DHS and ICE have relied on preexisting Privacy Act systems of records notices for the maintenance of records pertaining to law enforcement investigations performed by ICE. With the publication of the External Investigation Record System, DHS is consolidating and retiring two legacy U.S. Customs Service